Diversified Securities, Inc.

Written Supervisory & Control Procedures Manual

November 2015

DIVERSIFIED SECURITIES, INC.
Home Office Manual

Table of Contents

DIVERSIFIED SECURITIES INC.
Home Office Manual

Chapter One

1.00 Supervisory Control Structure

1.10 Introduction

Diversified Securities Inc. (hereinafter DSI) is a broker-dealer, incorporated in the State of California. Business activities are subject to the rules and regulations of the Financial Industry Regulatory Authority (FINRA); the Securities and Exchange Commission (SEC); and the state of California securities agencies. The firm is fully covered by the Securities Investors Protection Corporation (SIPC).

The OSJ Home Office location is at 6700 E. Pacific Coast Highway, Long Beach, California 90803. The telephone number is (562) 493-8881. The fax number is (562) 493-9352.

This Supervisory Procedures Manual, hereinafter, The Home Office Manual, documents the firm's system of supervisory controls and procedures, specifically the Principal Review and Approval process for all aspects of the firm's operations. Designated Home Office Principals are required to read this Manual and subsequent amendments carefully and adhere to the established supervisory procedures and controls. Please direct any questions or concerns about the Home Office Manual to your Supervisor or the Compliance Department for resolution.

In conjunction with the policies and procedures set forth in this Manual, it is expected that the Home Office Principals will exercise common sense, taking into consideration the factors that are unique to DSI, it's branch offices and/or the individual Registered Person. The true test of effective supervision is conducting business in a "reasonable manner" in light of the particular facts and circumstances surrounding a situation, and in compliance with the firm's procedures and industry rules and regulations. Effective supervision begins with good documentation.

Registered Representatives are also required to have a copy of this Manual, or access to it at all times and to be familiar with its content. All RRs and other associated persons at DSI are required to sign & return the acknowledgement included in this Manual.

It should be noted that this Manual includes only those rules, regulations & policies that are considered to be most applicable to supervision of the day-to-day activities of DSI's representatives & other associated persons. It is not all-inclusive of the laws & regulations with which the Company & its associated persons must comply. In order to be specifically familiar with the many rules & regulations affecting registered & non-registered personnel, DSI personnel are encouraged to visit FINRA Regulation Website at www.finra.org, especially the Information for Brokers page.

Approved Business: At this time, all of the Registered Persons of DSI are dually registered with the broker/dealer, H. Beck, Inc., hereinafter HBI, and DSI.

A. The DSI registered persons who are registered and approved by HBI may engage in the business as authorized and stated by HBI, and shall be governed by the rules & regulations of HBI. At this time the business of HBI, includes stocks, bonds & other securities trade execution services & offers annuities, direct participation programs, IRAs, government bonds, margin accounts, money market funds, mutual funds, options, & private placements & public offerings.

B. DSI registered persons who are registered & approved by DSI, may engage in the business as authorized & stated by DSI and shall be governed by the rules & regulations of DSI. At this time, the business of DSI is limited to the direct participation programs, hereinafter " DPPs" of the DSI Realty Funds. Should DSI wish to change the nature of its securities business outside the scope of approved business as described in its Membership Agreement, it will request & obtain prior FINRA approval.

DSI is not a market maker. The clearing function of its DPPs – the DSI Realty Funds, is accomplished by DSI's affiliate, DSI Properties, Inc.

New Programs/Products

At the present time, no new programs of the DSI Realty Funds are planned or anticipated. The B/D functions of DSI are presently limited to servicing the existing clients of the DSI Realty Funds for resales & registration changes. The company will ensure that no new programs/products are introduced to the marketplace before they have been thoroughly examined and sanctioned from a regulatory/business perspective. The CEO and CCO will have final authority to approve new products, & no products without this approval may be offered by DSI's Representatives.

1.20 Designation of Chief Executive Officer (CEO)

The firm's Board of Directors designates its Chief Executive Officer (CEO).

1.30 Designation of Chief Compliance Officer (CCO) & Executive Representative

The firm designates its Chief Compliance Officer (CCO) as the person to design, record and maintain the firm's system of supervisory control and procedures. The CCO is also nominated as the firm's Executive Representative.

1.40 System of Supervisory Controls and Procedures

Specific supervisory control procedures are considered and recommended to the firm by the CCO as required by FINRA Rule 3120, the Executive Vice President of Administration (hereinafter referred to as the EVPA); the COO and other qualified Principals. The Executive Vice President of Administration & the COO are closely involved with the formulation of supervisory control procedures, and provide guidance on the risk assessment and other assumptions made by the CCO.

The CCO is supervised by the CEO to ensure direct reporting of compliance matters of importance to the firm.

The firm's system of supervisory controls and procedures are published in the following documents:

- DSI's Supervisory Procedures Manual, aka "The Home Office Manual.".
- Written notices and other publications (Supplemental Writings).

1.50 Designation of the OSJ Home Office Principal

The EVPA is the firm's designated OSJ Home Office Principal.

1.60 Designation of Home Office Principals

In the capacity of OSJ Home Office Principal, the EVPA has authority to designate Home Office Principals to supervise all aspects of the firm's operations. The EVPA supervises the daily activities of each supervising Home Office Principal, and maintains regular and frequent contact with the firm's Department Managers.

The current designations of Home Office Principals are shown on Exhibit 1 entitled, "*Home Office Supervisory Principals*." The list shows the titles, registration status, dates duties assumed and reporting structure.

1.70 Approval and Adoption of the Supervisory Control Procedures

The CEO approves the adoption of the written supervisory control procedures and any subsequent amendments.

CEO Authority

The CEO reserves final authority over all written supervisory controls & procedures on any matter of significant importance or in situations of internal disagreement between DSI Principals over accepted written supervisory controls and procedures.

1.80 Review of Written Supervisory Control Procedures

No less than annually, the firm's written supervisory controls and procedures are reviewed by the CCO, in consultation with the COO, the OSJ of the Home Office and other Home Office Principals. This annual review process allows for a regularly scheduled time to evaluate the existing written procedures, and to identify any outstanding issues or questions involving current firm policy and practices. The review will include a written report of the following:

- A description of DSI's system of Supervisory Controls (i.e. a copy of this Manual)
- Summary of test results and an assessment of the Supervisory System
- Conclusions of Home Office and Branch Inspections
- Any steps taken to amend procedures.

A copy of the written report will be maintained in the CCO's files.

1.90 Implementation of Home Office Manual

The Home Office Supervisory Principals will assist with the implementation and practice of the firm's policies and procedures contained in this Manual. In addition, the Principal OSJ will communicate the importance that Home Office Principals be familiar with the procedures assigned to their supervision and be aware of any subsequent amendments to this Manual. Home Office Principals shall maintain a copy of this Manual at their desk for easy reference and an electronic copy will be maintained on the home office's computer network.

1.95 Distribution of Home Office Manual and Amendments

Distribution of Home Office Manual and Amendments

Promptly after adoption of this Home Office Manual, and all subsequent amendments, the assigned Compliance Staff will send an email to all Supervisors of Home Office Principals announcing its adoption. Notice also may be publicized by distribution of hardcopies, or any other appropriate means.

Supervisors at other DSI locations shall ensure that they have access to the Home Office Manual.

Recordkeeping

The assigned Compliance Staff will distribute the initial copy of this Home Office Manual and future amendments as specified above, and will keep a record of such distribution.

Chapter Two

2.00 Administrative Controls

2.10 Maintenance of Form BD/BR

The firm maintains a current Form BD/BR with FINRA and all state and regulatory agencies in which it conducts business that accurately reflects business activities and personnel. The firm also maintains current information on Form BD/BR for each registered Branch Office location. The requirements for each jurisdiction are met by initial filings, annual renewals, and amendments as necessary.

The Director of Licensing assures that the firm's Form BD/BR is current and electronically filed in a timely manner via the FINRA/CRD system

Approval of Amendments

Prior to filing any Form BD/BR amendment, the CCO and/or the COO review the proposed amendment. Evidence of this review is noted in writing by initialing and dating a hardcopy.

Annual Review

No less than once a year, the current Form BD/BR is reviewed by the CCO in consultation with the COO to verify its accuracy. Evidence of this review is noted in writing by initialing and dating a hardcopy.

Recordkeeping

The Director of Licensing maintains all records regarding Form BD/BR, including:

- Confirmed hardcopies of any amendment filings with FINRA/CRD;
- Approval of any amendments;
- Evidence of review; and
- The firm's complete Form BD/BR filing history.

2.20 Regulatory Reporting of Key Contacts

Under the supervision of the COO, the Director of Licensing reviews and reports the firm's Key Contacts in accordance with FINRA Conduct Rule 1150.

Timing Requirements

The reporting of Key Contacts is amended on an "as needed" basis. In addition, the Director of Licensing reviews the entire listing of Key Contacts within 17 business days after the end of each calendar quarter.

Recordkeeping

The Director of Licensing maintains the records in accordance with SEC Rule 17a-4. The firm's records include confirmed hardcopies of all filings and evidence of review.

The Director of Licensing also maintains written instructions for logging on to the FINRA website and entering the Key Contacts information.

2.21 FINRA Electronic Reporting

Under the supervision of the CCO or designee, the Director of Licensing is responsible for all electronic filings submitted via FINRA's Firm Gateway/CRD Systems. All submissions must be approved by a supervising principal prior to submission. These approvals are evidenced by the supervisor's initials on the file copy which is retained.

Louisa Gac has been designated as the firm's Super Account Administrator (SAA) with entitlements to create account administrators and user accounts, as well as manage access to FINRA regulatory systems.

2.22 MSRB Reporting

Diversified Securities, Inc. currently does not execute or facilitate any bond trades due to its self-limited business model. As a result of corporate restructuring, DSI terminated its MSRB membership in October 2007.

2.30 Fingerprint Card Filing

Registered Persons

To complete the registration process, a prospective Registered Person must submit a fingerprint card to the Director of Licensing. See Chapter 3 of this Home Office Manual (the Registration Process).

Unregistered Persons

As required by SEC Rule 17f-2, any unregistered associated person who handles customer checks, or posts entries to books of original entry, must submit a fingerprint card to the Director of Licensing.

The firm's policy is that **all** branch office personnel, regardless of their position, be fingerprinted.

Supervision

The COO (or designee) supervises the fingerprint card filing requirement and is immediately notified by the Director of Licensing of possible undisclosed conflicts with law enforcement agencies for appropriate action and resolution. The COO notifies the CCO of the disposition of these matters.

Recordkeeping

The Director of Licensing maintains records of fingerprint filings made to FINRA.

2.40 Maintenance of Form U-4 and Related Records

Registered Persons

The Director of Licensing maintains all internal records, agreements, CRD filings, and other available documents in individual files for each Registered Person. The CCO (or designee) supervises the maintenance of records for Registered Persons.

Under the supervision of the COO, the Director of Licensing coordinates addressing outstanding issues with the various regulatory agencies affecting the registration process. See Chapter 3 of this Home Office Manual (the Registration Process).

Unregistered Employees

Individual records of all DSI unregistered employees are located at the Home Office and are maintained by the firm's Human Resources Department. The records are available for inspection upon request by the CCO (or designee).

Form U-4

Upon affiliation with the firm, the Director of Licensing ensures that the Form U-4 is filed via the FINRA/CRD system to complete the registration process.

Form U-4 Amendments

During the annual renewal process, the Registered Person confirms basic information the firm maintains about their registration status.

The CCO and/or COO review and evaluate items that may require disclosure amendments to Form U-4 as a result of recent regulatory or legal action and/or customer complaint. Within 30 days of discovery by the firm, the Director of Licensing files required disclosure amendments to Form U-4 via the FINRA/CRD.

Form U-5

The Director of Licensing files Form U-5 with the FINRA/CRD system within a 30-day period of receipt of written notice from the Registered Person to terminate his or her registration.

The CCO, COO, or CEO authorizes the termination of registration of a Registered Person "For Cause," or other appropriate reason.

Once the Form U-5 has been submitted to the FINRA/CRD system for processing, the Director of Licensing (or designee) sends written notification of termination of registration, including a copy of the Form U-5, by c*ertified mail* to the Registered Person within the 30-day period of filing Form U-5 with the FINRA/CRD system.

Any subsequent amendments to Form U-5 are handled in the same manner as the initial filing.

The Director of Licensing maintains a copy of documentation of the Form U-5 in the separate individual files for each Registered Person.

2.50 Internal Compliance Training

The CCO (or designee) conducts periodic compliance training on a formal or informal basis for selected Registered Persons. Additional compliance training and other informational material about the firm's system of supervisory controls and procedures is provided in written form.

2.60 Investment Advisors

Diversified Securities, Inc. currently does not execute or facilitate any investment advisory business given its self-limited business model.

Chapter Three

3.00 Registration and Branch Office Organization

3.10 The Registration Process

The Director of Licensing (or designee) collects, tracks, and maintains the records associated with the investigation of the background of each prospective Registered Person ("Applicant"). The background investigation process is under the supervision of the CCO and COO.

Each Applicant is carefully pre-screened by the firm to determine the merits of a business relationship. Next, the Applicant undergoes a formal background investigation to allow the firm to review and evaluate his or her FINRA/CRD records, involvement with outside business activities, communications from the former broker/dealer, and any related disciplinary disclosure or other relevant items.

Disciplinary history includes: 1) being charged or convicted of any felony or a misdemeanor involving theft, fraud, investment or investment related activity, bribery, perjury, forgery, counterfeiting, extortion, false statements or omissions; 2) any disciplinary matters involving a regulatory agency; 3) a client complaint; 4) any liens or significant credit problems; and/or 5) bankruptcy.

Restriction

Until an Applicant receives formal notification of full registration from the Director of Licensing (or designee), the Applicant may not discuss, sell, or solicit business in any matter in connection with Diversified Securities, Inc.

Dual Registration

DSI allows dual securities registration solely and exclusively with H. Beck, Inc., an introducing broker/dealer based in Bethesda, MD. No exceptions to this policy are currently permissible.

Pre-hire Process

The firm employs the following pre-hire procedure to review, evaluate and register an Applicant.

1. The Applicant signs a general release authorizing the firm to conduct the background check.

2. The Licensing Department compiles the required registration documents, such as Form U-4, background report of legal proceedings, the firm's Outside Business Activities Disclosure Form and other relevant information. This information is organized and placed in the Applicant's file.

3. The Applicant's individual file and the supporting documentation is reviewed by the COO, CCO and other selected senior staff members.

4. Any record of disciplinary history or other types of questionable disclosure issues is carefully reviewed and evaluated. If the circumstances are judged to be material in nature, the firm may seek additional information (including an interview with the Applicant and/or other informed parties) so all relevant information can be considered.

5. During the course of investigation the firm may withdraw any consideration for registration if the background investigation reveals any unreported events and/or regulatory actions, or for any other reason as determined by the firm.

6. In accordance with SEC requirements, fingerprint cards are submitted to the FINRA for verification. See Chapter 2 of this Home Office Manual.

7. At the conclusion of the background investigation, the firm may accept or reject the request for registration, or impose Heightened Supervision requirements or other restrictions.

8. Once the Applicant is approved for registration, he or she must sign and submit additional internal documents, which are then placed in the individual's file. Among other things, these documents serve as evidence that the Applicant understands important firm policies.

9. After the required documents are received and reviewed for completion, the Licensing Department submits the registration for processing by the FINRA/CRD and each state(s) in which the Applicant will solicit clients or conduct business.

10. Once the registration is finalized and effective, the Licensing Department notifies the Applicant and Key Staff.

Post-Registration Background Information

The firm may rescind an acceptance of a request for registration and terminate a Registered Person's association with the firm based on background information obtained by the firm after registration.

Screening Process for Clerical and/or Administrative Applicants

The firm strictly prohibits the hiring of any person deemed to be "Statutorily Disqualified". Prior to hiring any clerical or administrative applicant the firm conducts a background check to determine if an applicant is not "Statutorily Disqualified" as defined by FINRA Rule 9520 and Section 3(a)(39) of the Securities Exchange Act of 1934. If the firm becomes aware of a statutory disqualifying event related to one if its employees it shall be reported to FINRA immediately by the CCO upon discovery.

3.20 Designation of a Branch Office

Branch Office Designation

The Branch Office registration process is under the supervision of the COO. All Branch Offices are designated as Non-OSJ Branch Offices, unless the COO or CCO otherwise specifies.

Office of Supervisory Jurisdiction (OSJ) Designation

The COO or CCO may designate a Branch Office as an Office of Supervisory Jurisdiction (OSJ).
Unless agreed to in writing by the firm, NO Principal Review and Approval functions are conducted at the Branch Office locations.

Note: The Home Office is an OSJ, although the firm refers to it simply as the Home Office.

Designation of Non-Branch Office

FINRA Rules allow a Branch Office location an exemption from the filing requirements associated with Form BR, known as a Non-Branch Office. As a matter of policy the firm does NOT allow Non-Branch Office designations.

Branch Office Inspections

The firm's Branch Office Inspection Program is an integral part of the firm's overall supervisory control procedures. These onsite inspections by the Compliance Department are designed to verify that the firm enforces established compliance procedures in the same manner as regulatory examiners. This inspection process also provides the firm with an opportunity to determine the existence of unknown (unreported) compliance concerns, and to take any appropriate corrective action to ensure that the firm's compliance procedures are followed and to prevent the possible occurrence of sales practice problems or customer complaints.

The Compliance Department visits each Branch Office location annually or bi-annually, depending on a number of factors, such as office size, volume of activity, production, complaints or possible sales practice violations, unusual trading activity, and the

number of Representatives. FINRA requires that a number of Branch Office Inspections be conducted each year on an unannounced basis.

At the conclusion of the inspection, the Compliance Examiner discusses the findings and provides a written Exit Interview Form describing any concerns noted. Depending of the specific findings, the Exit Interview Form may require additional corrective action by a specified date.

If the inspection findings result in significant recordkeeping or other sales practice concerns, the Branch Office location may be subject to semi-annual inspections or other special considerations at the discretion of the CCO.

During subsequent inspections, the Examiner will review the items noted in the previous year(s) to ensure that the Branch Office corrected all deficiencies and that none are repeated. Failure to implement the agreed upon corrective actions recommended during the previous Branch Office Inspection may result in additional enforcement actions, as determined by the CCO.

Items Reviewed During a Branch Office Inspection

The Branch Office should expect the following records to be reviewed during a Branch Office Inspection.

Required Blotters/Logs (Must show all daily activity)
- Trade Blotter
- Check Blotter
- Securities Receipt Blotter

Required Centralized Files (Maintained, even if empty)
- Advertising & Sales File
- Correspondence File (Incoming and Outgoing)
- Complaint File
- Gift & Gratuity File
- "Do Not Call" File
- Annual Privacy Notice File
- Compliance File
- Sampling of client files (selected by Examiner)

Other Compliance Matters
- Signage
- Outside Business Activities Form
- Personal Brokerage Account Form
- Internet access to the firm's website for Manuals and other information
- Bank Accounts

Recordkeeping

Branch office inspection findings and reports are maintained by the CCO.

The Director of Licensing (or designee) records and preserves Form BD/BR for each registered Branch Office via the FINRA/CRD system. See Chapter 2 of this Home Office Manual.

The Director of Licensing (or designee) maintains a current list of each OSJ Branch Office location and each OSJ Supervisor.

3.30 Designation of the Supervisor

In accordance with FINRA requirements, the firm must designate a qualified Supervisor to supervise the various activities of the Registered Persons associated with the Branch Office. The Supervisor is responsible for conducting specific tasks identified in writing by the firm.

The designation of Supervisors process is under the supervision of the COO. The COO (or designee) verifies that each Supervisor is qualified according to the requirements established below. The COO (or designee) may subsequently modify the designation of any Supervisor and/or the assignment of Registered Persons to a Supervisor.

Classification of Supervisor (Types)

Depending on location, the Diversified Securities, Inc. Supervisor is classified as follows:

- Branch Supervisor (Non-OSJ Branch Office); or
- Home Office Supervisor (OSJ Home Office).

These internal classifications (types) do not alter the specific supervisory tasks and responsibilities common to all Supervisors.

Mandatory Limitations

Four critical requirements apply to the firm's assignment of Supervisors:

1. No Supervisor may supervise his or her own activities. In other words, *no self-supervision* is allowed by the firm.

2. Single-person Branch Offices *must* be assigned to a Home Office Supervisor, since no self-supervision is allowed by the firm.

3. To supervise the activities located in an *offsite* Branch Office location, a Supervisor must be FINRA-qualified as a Series 24 or 26.

4. Every DSI Registered Person *must* be assigned to a Supervisor.

Notice of Designation and Assignment

At the time of designation, the Director of Licensing (or designee) provides written notice to the Supervisor of the designation and the names of the Registered Persons assigned to the Supervisor. At the same time, the Registered Persons are given written notice of his or her assignment to the Supervisor.

Recordkeeping

The Director of Licensing (or designee) maintains a current record of the designated Supervisors.

Ongoing Evaluation

The COO and/or CCO may evaluate the Supervisor's performance at any time for any reason. Prompt evaluation is given in the following situations:

- Qualifications as specified above are questioned
- By request of management
- Significant compliance problems generated from a Branch Office location
- Failure to maintain effective compliance practices
- The firm has notice of any other relevant information.

Replacements

The COO may replace a designated Supervisor as circumstances require. The COO (or designee) promptly assigns a replacement Supervisor whenever a Supervisor is replaced or is no longer associated with the firm. The Director of Licensing provides notice of the replacement.

3.40 Assignment of Registered Persons to Supervisor

In accordance with FINRA requirements, the firm must assign each Registered Person to a qualified Supervisor. During the Pre-hire process, the COO (or designee) assigns a Supervisor to each Registered Person. The COO may seek recommendations and input from the CCO, senior management or other staff regarding the assignments.

Reassignments

The COO (or designee) may reassign a Registered Person to another Supervisor as circumstances require. The Director of Licensing provides notice of the reassignment.

Review and Approval Procedures

Each Registered Person and Supervisor will continue to be subject to the firm's system of supervisory control and procedures requiring Principal Review and Approval. The firm's Review and Approval procedures are covered elsewhere in this Home Office Manual.

Recordkeeping

The Director of Licensing (or designee) maintains the assignment of each Registered Person to a designated Supervisor.

Chapter Four

4.00 Compliance Controls

4.10 Outside Business Activities

FINRA Rule 3270

FINRA Rule 3270 dictates that a Registered Person shall not be employed by, nor accept compensation from, any other person as a result of any business activity (other than a passive investment) outside the scope of his or her relationship with their broker/dealer, unless the Registered Person has provided prompt written notice to his or her broker/dealer.

Duty to Disclose

Registered Persons have an ongoing obligation to promptly disclose all outside business activities to the Compliance Department before engaging in the activity.

Both the initial disclosure information and any subsequent modifications must be in writing. Registered Persons must obtain an "OBA" form from the Compliance Department.

Compliance Department Review

Upon receipt of notice of an outside business activity from a registered representative, the firm will determine whether the proposed activity would (i) interfere with such registered representative's responsibilities to the broker-dealer and/or its clients or (ii) be viewed by clients or the public as part of the broker-dealer's business.

The disclosed activity is reviewed by the assigned Compliance Staff for conflicts of interest with DSI's policies and business practices. In general, the firm determines whether an activity relates to private securities transactions or other prohibited activities, or otherwise raises concerns. The firm reserves the final authority to prohibit any outside business activity or private securities transaction proposed by the Registered Person.

The assigned Compliance Staff will notify a Registered Person whenever a disclosed outside business activity cannot be approved. Otherwise, it is not necessary to notify the Registered Person of review of the disclosed outside business activity.

Recordkeeping

The Licensing Department maintains the OBA records and attestations regarding private securities transactions in the individual Registered Persons files.

Securities Accounts. All personnel must advise the Company of all accounts in which they may transact in securities. The Company does not as a matter of policy permit any Registered Representative or employee to maintain a securities account with an outside broker-dealer without express prior written permission of the designated Principal. This does not apply to accounts maintained directly with mutual fund sponsors.

Trading. In transacting business for themselves all Company personnel must observe principles of conduct announced in this Supervisory Procedures Manual and elsewhere by the Company in order to foster professionalism and integrity in the Company's business.

4.20 Annual Regulation SP Privacy Notification

DSI's Privacy Policy and any updates thereto are available on the firm's website at www.divsecs.com.

4.30 Continuing Education Program – Firm Element

Currently, the Firm Element CE Program is a web-based training program that offers individual training modules (courses) on specific topics associated with investment products and services, general sales practice issues, and ethical business behavior.

Firm Element CE Program Notices

During the first quarter of the year, all current Registered Persons are provided with written notice of annual CE Program requirements and details on participating.

Deadline

The annual requirement must be satisfied on or before December 31, unless extended by the CCO on a case-by-case basis.

Failure to Complete Firm Element CE Program

Once the established deadline for completion of the Firm Element CE Program has lapsed and all reasonable efforts to accommodate and assist the Registered Person to fulfill the requirement have been exhausted, the CCO refers the matter to the CEO, who after consultation with the CCO and the Home Office OSJ, takes appropriate action to enforce the requirement, including termination of the Registered Person's securities registration.

Recordkeeping

The assigned Compliance Staff maintains the annual Firm Element CE Program records, including completion, exemption, waivers and delinquencies. The assigned Compliance Staff also maintains the records documenting the assessment, design and content of the annual CE Programs.

4.40 FINRA Continuing Education – Regulatory Element

The required Regulatory Element of the FINRA CE Program is under the supervision of the Home Office OSJ.

Regulatory Element Anniversary Date

The Regulatory Element must be completed within 90 days of the anniversary date established by the CRD/FINRA for a Registered Person and every third year thereafter.

Regulatory Element Contact Person

As part of the FINRA Contacts quarterly review, the Director of Licensing (or designee) reviews and updates, if necessary, the information regarding its Regulatory Element contact person(s) within 17 business days after the end of each calendar quarter to ensure the information's accuracy.

Notification Process

As applicable, the Licensing Department sends advance written notice to each Registered Person pertaining to FINRA Rule 1120 and providing the "window" dates (a three-month period) for taking the Regulatory Element course. The Licensing Department also sends one or more reminder notices to the Registered Person.

At the request of the Director of Licensing (or designee), the CCO (or designee) at any time may contact a Registered Person to explain the Regulatory Element requirement, or otherwise attempt to assist with satisfying the requirement.

Whenever a Registered Person has less than 30 days to complete the Regulatory Element, the Director of Licensing (or designee) will refer the matter the CCO (or designee) for enforcement of the requirement.

Failure to Complete Regulatory Element

If the Registered Person fails to complete the Regulatory Element within his or her specified timeframe, their registration automatically immediately becomes inactive with the CRD/FINRA.

It is the general policy of the firm to not indefinitely maintain the registration of the Registered Person who fails to satisfy the Regulatory Element within the required timeframe specified by FINRA, unless the CCO, in consultation with the COO and Home Office OSJ, determines otherwise. The Home Office OSJ establishes a specific deadline for completing the Regulatory Element for any Registered Person who becomes inactive. The Registered Person and his or her Supervisor are given written notice of the deadline. This deadline is monitored by the Compliance and Licensing Departments. The CCO notifies the Home Office OSJ and the COO if additional action becomes necessary, including termination of the Registered Person's securities registration.

IMPORTANT: Any person whose registration becomes inactive must cease ALL activities, duties and functions requiring registration. An inactive person may not be paid commissions, generate business, nor make any transactions on a client's account. If the Registered Person becomes active again, they may not be paid for any commissions relating to transactions made by any client during the period in which the Registered Person's registration was not active.

Recording and Announcing Inactive/Active Status

Whenever a Registered Person becomes inactive, the Licensing Department immediately notifies the COO, EPVA & CCO and the inactive representative notifying them that the inactive person will not be permitted to transact business and/or receive commissions during the inactive period.

Recordkeeping

The Director of Licensing (or designee) maintains the firm's Regulatory Element CE records, including copies of any termination notices.

4.50 Gifts and Gratuities

Pursuant to FINRA Conduct Rule 3060, the firm prohibits all Registered Persons from giving or receiving gifts or gratuities of any kind related to the business of the firm, unless the value does not exceed $100 annually, and is judged to be customary, reasonable, and proper under the circumstances. A gift of any kind is considered a gratuity.

Rule 3060 does not apply to: (1) contracts of employment with or to compensation for services rendered by persons, (2) an occasional meal, a ticket to a sporting event or the theater, or comparable entertainment which is neither so frequent nor so extensive as to raise any question of propriety and is not preconditioned on achievement of a sales target (e.g., non-cash compensation), and (3) reimbursements by a Registered Person of a client's expenses when the reimbursement is unrelated to the business of the client's employer.

Reporting Gifts and Gratuities

Registered Persons must submit their written requests for approval of gifts or gratuities in any amount to the Compliance Department. Such decisions are made on a case-by-case basis, and any approval shall be evidenced in writing. In no instance will any such gifts be permitted to exceed $100 for any one individual over a 12-month period.

The CCO (or designee) records approved gifts and gratuities in a centralized log maintained by the Compliance Department.

4.60 Prohibited Business Activities

The firm's Prohibited Sales Practices are listed in DSI's Compliance and Procedures Manual and are designed to eliminate the most questionable types of client activities or conflicts of interest and thereby reduce potential problems associated with "just and equitable principles of trade."

Lending with Clients

A Registered Person may not make loans to clients, accept loans from clients, nor arrange for any personal financing for clients without prior written permission from the CCO, COO or the Home Office OSJ Principal.

Sharing in Client Accounts

The sharing of profits or losses in an account with a client is prohibited.

Prohibition Against Guarantees

DSI strictly prohibits the "guaranteeing" of any market performance or against losses to clients, either in writing or orally.

Parking of Securities Registration

A Registered Person may not maintain a registration with the FINRA/CRD when he or she is no longer functioning as a representative, or where the sole purpose for registration is to avoid the lapse of FINRA examination qualifications that may result from termination of the registration. This is commonly called "parking of securities registration," and is a violation of FINRA Rules.

This prohibition does NOT apply to a Registered Person who performs legal, compliance, internal audit, back-office operations, or similar responsibilities for the firm, or who performs administrative support functions for a Registered Person.

Unauthorized Transactions

A Registered Person is prohibited from causing the execution of transactions which are unauthorized by the client or the sending of confirmations in order to cause clients to accept transactions not actually agreed upon.

Insider Trading

Employees and representatives are strictly prohibited from effecting transactions based on knowledge of material, non-public information.

It is the policy of the Company that all personal trades by Registered Representatives and employees must be pre-approved by the supervising Principal and such approval noted on the order ticket. The Principal designated to approve and review personal accounts and trading is also required to comply with these procedures. Approval of, and subsequent review of, personal accounts and trading are the obligations of the EVPA. This designated individual must ensure that the policies described above are enforced and documented and must document and follow up on any violations discovered.

Chapter Five

5.00 Evaluation of Supervisory Control Procedures

5.10 Designation of Principal Capacity

Chief Compliance Officer

The firm has designated the CCO as the principal responsible for recommending, maintaining, and enforcing the firm's system of supervisory controls and procedures.

Chief Operating Officer/Executive Vice President of Administration

On behalf of the firm, the COO, in consultation with the EVPA, authorizes and accepts specific supervisory controls and/or amendments as recommended by the CCO. This second review and approval process for supervisory control procedures offers the firm and the CCO the following important advantages:

1. Guidance and assistance from executive level management;
2. A standard method to introduce and approve amendments pertaining to compliance and supervisory control procedures;
3. A means to ascertain how business policy positions impact supervisory controls; and
4. Increased authority and support for enforcement of the firm's compliance and controls procedures.

The COO consults regularly with the CCO to discuss updates on compliance projects/assignments and other compliance issues of concern. The COO communicates these findings to the CEO and EVPA as necessary.

The firm has designated the EVPA as the principal responsible to certify annually that the firm has in place processes to establish, maintain, review, test and modify written compliance policies and written supervisory procedures reasonably designed to achieve compliance with applicable FINRA and SEC rules and regulations.

5.20 Testing of Supervisory Control Procedures

The CCO (and designees) conduct annual testing to verify that the supervisory control procedures are "reasonably designed" to achieve compliance with applicable FINRA rules and internal compliance procedures. The CCO evaluates the findings of the firm's internal testing in conjunction with any other known compliance risks, new business lines for the firm, or any new FINRA/SEC rules applicable to the firm's operations.

The evaluation process may result in the recommendation to be considered by the firm to eliminate or amend existing supervisory control procedures and/or create new supervisory control procedures.

5.30 Annual Compliance Report of Supervisory Control Procedures

Annually each December 1, the CCO prepares a formal written Compliance Report of Supervisory Control Procedures for the CEO, EVPA and COO which summarizes the findings resulting from the testing and evaluation of the firm's supervisory control procedures. This Report may include specific recommendations to strengthen existing supervisory control methods, adopt an action plan to institute corrective action for significant identified exceptions, and/or create additional or amended supervisory procedures in response to the test results.

The Compliance Report of Supervisory Control Procedures is regarded as a primary source document that serves as a basis for the CEO's Annual Compliance and Supervision Certification.

5.40 Annual Compliance and Supervision Certification

Annually each December 1, the CEO certifies in writing that the firm has in place processes to establish, maintain, review, test and modify written compliance policies and written supervisory procedures reasonably designed to achieve compliance with applicable FINRA rules and SEC laws and regulations.

No less than annually, one or more meetings to discuss these processes are held with the following parties, and any additional staff included at the firm's discretion:

- EVP of Administration;
- Chief Operating Officer; and
- Chief Compliance Officer.

The stated objectives of the meeting(s) include, but are not limited to:

1. Discuss and review the matters that are subject of the annual certification;

2. Discuss and review ongoing compliance efforts and measure progress;

3. Identify and address significant compliance exceptions; and

4. Report the status of ongoing compliance priorities, accomplishments and/or resource needs.

Additional items of interest may be addressed at the discretion of each meeting attendee.

Recordkeeping

The CCO maintains the documentation associated with these meetings, including the parties attending, and the dates and times the meetings were held.

Chapter Six

6.00 Communications with the Public

6.10 Summary of Communications with the Public

The CCO (or designee) supervises the review and approval of investment-related communications with the public. Unless otherwise specified, all forms of communications with the public regarding DSI Realty DPPs must be approved by the firm prior to first use.

Common forms of communications with the public include sales literature, advertising, seminars, direct mail, public speaking, customized client account statements, and internet websites.

6.20 Definition of Communications with the Public

Listed below are the three media classifications generally used to communicate with the public.

Advertising

The use of advertising is a type of communication delivered to an *unknown* audience.
Common types of advertising include:

- Newspapers;
- Magazines or other periodicals;
- Radio;
- Television;
- Books about investing;
- Telephone hold or tape recordings;
- Video tape displays;
- Signs or billboards;
- Motion pictures;
- Telephone directories (Yellow Pages);
- Electronic media (internet); and
- Other public media.

Sales Literature

The use of sales literature is a type of communication delivered to a *known* audience.
Business Cards and Stationery are considered sales material. Common types of sales literature include:

- Business Cards;
- Stationery;
- Circulars;
- Research Reports;
- Customized Client Account Statements;
- Market Commentary Letters;
- Performance Reports;
- Form Letters sent to 25 or more prospective retail customers (if under 25, the letter is correspondence);
- Public Speaking;
- Cold Calling;

- Seminars;
- Reprints or excerpts of published articles; and
- Sponsor-prepared materials.

Correspondence

The use of correspondence is a type of communication delivered to a known audience of existing clients and less than 25 potential retail clients.

Common types of correspondence include:

- Letter;
- Electronic communication (e-mail); and
- Faxed materials.

Correspondence should not be product specific. The sales presentation should occur during a face-to-face meeting with the client at which time all material information is discussed. Sending prospectuses and pre-approved sales material with the intention of discussing the material in person is permitted, so long as the correspondence makes this intent clear.

6.30 Review and Approval of Advertising and Sales Literature

Requirements

Advertising, sales literature and emails delivered to more than 24 potential retail clients must be submitted to the Compliance Department in advance. All other correspondence is subject to "post-review" and is examined by a Compliance Principal during inspections, or through spot checks conducted by the Compliance Department from the Home Office.

Review and Approval

After review of items requiring pre-approval, the assigned Compliance Staff sends written notice of approval to the Registered Person. If the material is not approved, the assigned Compliance Staff contacts the Registered Person and discusses the matter. The firm does not approve material on a conditional basis. Revised material must be re-submitted for review in the same manner as original submissions.

Recordkeeping

The assigned Compliance Staff maintains the records of review and approval of communications with the public. The Registered Person must also maintain an Advertising/Sales Material File at his/her Office location.

6.40 Review and Approval of Correspondence

Incoming Correspondence

Home Office

All mail is opened immediately upon receipt to assure that correspondence is promptly forwarded to the proper area for WSP/WSCPs complaint or regulatory inquiries are promptly routed to the Compliance Department. Incoming correspondence is under the supervision of the COO.

Branch Office Locations

Branch Office Locations open incoming correspondence and follow the same procedures as the Home Office. The Home Office provides training to any designee who is responsible for reviewing incoming mail.

Factors to Consider When Reviewing Incoming Correspondence

Incoming correspondence is considered for any possible customer complaints, money sent through the mails, or any unusual items. The designee brings these issues to the attention of the Supervisor and/or the Compliance Department. The Supervisor or Registered Person should advise the Compliance Department of any unusual items that may suggest violations of internal procedures or securities rules.

Complaint Matters

The person reviewing the incoming correspondence should immediately report all client complaint matters or client disputes to the appropriate Supervisor who will then notify the Compliance Department. If the Supervisor is unavailable, or for a single-person Office, the Compliance Department should be immediately notified.

Outgoing Correspondence

The firm allows for the post-review of outgoing correspondence with the exception of correspondence relating to the solicitation of a security transaction. As provided under Section 6.30 of this Home Office Manual, for this type of correspondence prior approval is required.

Examples of correspondence relating to the solicitation of a security transaction include text that suggests specific services available through the Registered Person's relationship with DSI.

Factors to Consider When Reviewing Outgoing Correspondence

Any communication that appears to suggest inappropriate sales practices should be investigated. It is also important to train the office personnel on the review procedures for sending out client correspondence. The Compliance Staff may conduct a spot check of correspondence. The Compliance Department reserves the right to reject any correspondence under its review.

The Branch Office location may maintain a centralized file for all outgoing correspondence requiring a review and approval prior to client use. Alternatively, correspondence may be maintained in individual client files. All other types of correspondence should be maintained in the client files and is subject to review.

Recordkeeping

Each Office retains correspondence for three years. The assigned Compliance Staff maintains copies of correspondence submitted to the Compliance Department for review, or otherwise reviewed by the Compliance Staff, for a period of three years.

Electronic Mail (E-mail)

E-mail communication is considered correspondence and is fully subject to the same review procedures as any other types of correspondence. DSI's procedures require that copies of all business-related email correspondence be maintained and available for review in the same manner as written correspondence.

As of December 2010, e-mail correspondence and archiving for our divsecs.com domain is conducted via our outside provider – Smarsh, Inc. (www.smarsh.com). The Smarsh hosted email archiving and email compliance solution captures every email (and attachment) that enters or leaves the organization, as well as internal messages, and preserves them all in evidentiary-quality form in a central repository (an email archive for email retention). All of the firm's reps are required to maintain and utilize a *name@divsecs.com* email for all business-related correspondence.

6.50 Speaking Engagements

Any Registered Person who plans to discuss the sale of securities at any public gathering must submit his or her outline, as well as any slides, advertisements, invitations and any investment-related sales literature or materials to be distributed, to the Compliance Department for review and prior approval. To facilitate the review, the assigned Compliance Staff may ask the Registered Person to complete a Speaking Engagement Form, or otherwise provide written details.

During the speaking engagement, the Registered Person should not deviate from the prepared outline. Prospectuses should be distributed at seminars if a specific product is discussed.

6.60 Telemarketing (Cold Call Rule)

A telephone solicitation (cold call) is a telephone call placed to a person with whom neither the caller nor the firm has an established business relationship, or one in which the person called has not given express written permission to call them.

Telemarketing scripts are sales literature subject to review by the Compliance Department. Prior to conducting a cold calling campaign, the Registered Person must submit a sample script, along with the hours of the campaign and the names of persons conducting the calls. The Registered Person may not use an automatic calling device, and may not have one present in his or her office.

Each Branch Office location is required to maintain a "Do Not Call" File. The Compliance Department maintains a Master "Do Not Call" List of persons not wishing to be contacted again. When a Registered Person receives a request to place a number on the firm's Do Not Call List, he or she must promptly notify the Compliance Department so that number can be added to the List.

6.70 Use of Third-Party Articles

The press or other media may write an article or run a story that references DSI or its DPP's. Use of such materials to support a sales effort, such as showing them to prospective clients or reproducing them for distribution to current clients, turns the article or story into sales literature that must be approved by the Compliance Department prior to use.

6.80 Performance Data

Data indicating past performance may be helpful in supporting certain marketing efforts. Since the public easily misunderstands past performance data, it is essential that this type of information be presented in a complete manner and that certain mandatory disclosures be included.

All materials discussing or showing performance of DSI's DPP's must be submitted to the Compliance Department for prior approval.

6.90 Testimonials

Special rules apply to testimonials (client or actor statements concerning the quality of a Registered Person or the firm), which must clearly state in the advertisements or sales literature or communication that:

- The testimonial may not be representative of the experience of other clients.
- The testimonial is not indicative of future performance or success.
- If more than a nominal sum is paid for the testimonial, the fact that it is a paid testimonial must be indicated.
- If the testimonial concerns a technical aspect of investing, the person making the testimonial must have knowledge and experience to form a valid opinion.

6.95 Internal Use Only Material

Communications sent to Registered Persons by Diversified Securities, Inc. or sponsor product vendors/wholesalers may be designated for "Internal Use Only," "For Broker/Dealer Use Only" or "Not for Use with the Public." Such material also may be found on sponsor websites in the registered representative only sections.

As indicated, the materials are for the Registered Person's information and edification only. FINRA restricts the material from being given to, shown to, or used with the public. A Registered Person must seek prior approval from the Compliance Department before cutting, copying, or altering this type of material for presentation to clients or potential clients.

6.96 Internal Communications

Books and records rules require maintenance of inter-office memoranda and communications relating to the Company's business. These requirements pertain to the record keeping of incoming, outgoing and e-mail correspondence and also apply to internal communications. Reviews of inter-office memoranda and communications are conducted randomly by the CCO and are evidenced by his or her initials and the date of review on copies or by other, electronic notation, if applicable.

Internal e-mail communication is considered correspondence and is fully subject to the same review procedures as any other types of correspondence. DSI's procedures require that copies of all business-related email correspondence be maintained and available for review in the same manner as written correspondence.

Internal e-mail correspondence is included as part of the periodic review by the firm's EVPA. Copies of all incoming and outgoing emails within the divsecs.com domain are cc'd to a compliance folder on the EVPA's computer in which it is reviewed. Once reviewed, the emails are marked electronically as read to evidence the process.

6.97 Prohibited Communications

Specifically, the firm prohibits the use of any of the following types of written electronic communications except for personal use only:

- Text Messaging
- Instant Messaging
- Message Boards
- Networking websites with Instant Messaging, such as Facebook, & MySpace.
- Twitter
- Web Blogs
- Podcasting
- Unapproved Email Communications
- Any other mode of written electronic communications.

The firm is required by the SEC and FINRA to supervise all investment-related communications (incoming and outgoing) and to evidence that supervisory reviews were actually conducted. The firm must prohibit the use of written electronic communications with securities clients and/or for the promotion of investments products and services with the public, except for approved email communications and websites, since by their very nature there is no feasible way for the firm to gain access and review historical records.

A Representative may use a networking website with Instant Messaging, such as Facebook, or MySpace for personal use only. "Personal use" means that there is no mention of investments and no links.

If the firm becomes aware that the Representative has used any form of unapproved electronic communications with clients and/or the public, the matter will be referred to the CCO for possible disciplinary action.

Chapter Seven

7.00 Client Account Information

7.10 New Account Form

General Requirements

The firm's standard New Account Form is required for each client account registration (e.g., individual, joint, IRA, trust, etc.) maintained by the firm.

The New Account Form must be signed by the client, the introducing Registered Person, and the designated Principal accepting the account on behalf of the firm. The client is provided a copy of the completed New Account Form for their records. The New Account Form must be accepted by the firm prior to the admission of a new limited partner.

7.20 DSI Account Agreement

Pursuant to SEC Rule 17a-3 and FINRA Rules, specific information must be provided to the client at the time an account is established with the firm. This information is provided in the Important Client Information section of DSI's Account Agreement, which contains the following key information:

- Information about the Customer Identification Program;
- Summary information Privacy Policy;
- Summary information about the Business Continuity Plan;

The Account Agreement is provided to the client by the introducing Registered Person at the time the account is established.

7.30 Required New Account Information

Basic client contact, suitability and other background information about the account holder must be provided on the New Account Form. The data contained on the New Account Form must be kept current since it is the primary source of information used in the determination of suitability of a transaction and the client's mailing address.

The specific client information and authorizations required to be completed on the New Account Form depend on the type of account being established with the firm.

Accounts

All accounts require the following information:

- Customer Name (including name of authorized person in the case of institutional accounts);
- Address (post office box is only accepted if accompanied by a street address);
- Social Security or Tax Identification Number;
- Date of Birth;
- Employment information;
- Customer Identification data;
- Number of Dependents;
- Annual Income;

- Tax Bracket;
- Net Worth exclusive of Home;
- Risk Exposure;
- Investment Objectives;
- Years of Investment Experience;
- Source of Funding; and
- Any other information necessary for making investment recommendations.
- The Registered Person also ascertains whether the customer is of legal age, an employee of the firm or another broker/dealer, or related to such an employee, and/or has a greater than 10% ownership in a publicly traded company.

Additional client account information that should be collected includes:

- Type of account;
- Nature of account (individual, joint tenants, etc.);
- Certificate transfer notice;
- Distribution payment instructions; and
- Home and business phone numbers.

The introducing Registered Person is strongly encouraged to seek any additional client documentation to assist in evidencing client suitability.

Transactions by an Associated Person

When a new account is applied for by an associated person of another registered broker dealer, the firm's Compliance Department will be notified by the SPVA.

The Compliance Staff notify, in writing, the associated person's affiliated broker/dealer and code the account for duplicate account information to be provided pursuant to their instructions.

Transactions Involving FINRA and American Stock Exchange Employees

In accordance with FINRA Conduct Rule 3090, the firm shall implement required written instructions from the employee of the FINRA/American Stock Exchange directing that duplicate account statements be provided to their employer. Offers by the firm of other types of consideration to these account holders are strictly prohibited.

7.40 OFAC Reporting

The Registered Person confirms that a new client account does not appear on any list of known or suspected terrorists or terrorist organizations such as those persons and organizations listed on the Treasury's Office of Foreign Assets Control (OFAC) website (www.treas.gov/ofac), and available on the firm's website home page under "List of Suspected Terrorists/Money Launderers" (SDN List), as well as the listed embargoed countries and regions (collectively, the OFAC List).

If a new client is found to have a match on the OFAC List, the Registered Person notifies the firm's AML Officers and the firm takes the following steps:

1. Freeze the funds of the individual
2. Place the funds in an interest bearing escrow account
3. Notify OFAC within 10 days of discovery
4. Notify client that funds have been frozen

7.50 Change of Address, Account Name and/or Investment Objective

The firm has designed supervisory control procedures to maintain strict control over any requests for change of address, name and/or investment objective for existing client accounts.

Before the firm considers a request for a change of address, name and/or investment objective for an account, the account holder or their representative of record must sign and submit a written request to the Home Office. The request is then reviewed and processed as detailed below.

Note: A change of account name includes personal name changes, such as change upon marriage or divorce, as well as a name change related to the account designation, such as a change in the named Trustee or beneficiary.

If the submission appears to be in good order and the address does not belong to the Registered Person, the account holder's request for a change of address is approved and retained then noted electronically.

The Firm provides written notification of the amended account information to both the old and new mailing address of the client to confirm that the change of address on the account has been completed. The client is also provided contact information to report any unauthorized change of address and to cancel the amended information.

Given the fact that DSI is currently a self-limited broker/dealer with only ONE product, changes in investment objective after the initial purchase are essentially immaterial. DSI's role in these transactions is solely to accommodate unsolicited sales of our affiliate's limited partnership units. When a potential buyer is acquiring units, investment objectives are considered during the initial suitability review. After purchase, changes in investment objective are irrelevant considering that these are one-time unsolicited principal transactions with limited liquidity.

7.60 Notification of Customer Identification Program ("CIP")

The client is provided written notification of the CIP when establishing an account with the firm by means of the DSI Account Agreement. The CIP requires the account holder to provide to the Registered Person a government-issued picture identification card as a source to verify the client's identity. The CIP requires the recording of the identification number, county or state of issuance, date of issuance, and date of expiration of the source document.

The required CIP information is recorded directly on the New Account Form and is under the supervision and enforcement of the DAS (or designees).

If the client refuses to provide the required CIP information, the firm will not open the account or process any transactions or deposits. Exceptions to this policy may be authorized by an AML Officer.

7.70 Notification of Investment Objectives

The required Investment Objective selection is recorded directly on the New Account Form and is under the supervision and enforcement of the DAS.

The Investment Objectives include the following selections:

Growth
Investor generally seeks capital appreciation through buying and holding securities over an extended period of time.

Income
Investor generally seeks current income over time.

Growth & Income
Investor generally seeks both capital appreciation through buying and holding securities over an extended period of time and current income over time.

7.80 Notification of Privacy Policy

The client is provided written notification of the firm's privacy policy when establishing an account with the firm by means of the DSI Account Agreement. In addition, the policy appears on DSI's web page and annually in reports to the DSI client household. The notification process is supervised in the daily course of business by the COO (or designee) and inspected by the CCO (or designee).

Chapter Eight

8.00 Supervision of Transactions

8.10 Designation of EVPA

All transactions are subject to a suitability review as part of the supervision of transactions conducted by the firm's EVPA.

The CEO designates the firm's EVPA. The current EVPA is listed in Exhibit #1 of this Home Office Manual.

8.20 Function of the EVPA

This Section describes the general procedures applied by the EVPA when conducting the firm's review and approval of transactions function.

The Registered Person must obtain specific financial information from the client, evaluate the client's investment goals and objectives, and establish the client's investment history and attitudes toward market and investment risks. This information is critical to the review of a transaction and forms the basis for the investment recommendations, and also provides the EVPA with necessary information to support the Registered Person's suitability determination.

When carrying out the review and approval function for the firm, the designated EVPA must:

1. Determine if the Registered Person is registered to offer the product or service in the client's state.

2. Possess a thorough knowledge of the specifications of the product being recommended.

3. Determine if sufficient client information is available to confirm an independent suitability determination for the transaction.

4. If necessary, exercise authority to question the Registered Person and/or Supervisor regarding incomplete or questionable items subject to review and approval.

5. If necessary, request assistance from the COO or other qualified Home Office Principal, including the CCO and/or DSI's General Counsel.

6. Utilize the exception parameters designed by the firm to screen both investors and transactions for additional suitability documentation and review and approval by the EVPA.

7. Exercise final authority to recommend a transaction, or if necessary endorse other appropriate corrective or enforcement actions.

8.30 Evidencing Client Suitability

Suitability is not an exact science. The firm recognizes the experience and professional judgment of the EVPA is the most important aspect of supervision of transactions. However, the evaluation of any transaction cannot be complete without adequate documentation to support the basis of the review process.

Commonly accepted forms of documentation that serve as a basis for evidence of the suitability determination include, but are not limited to, the documents described below.

New Account Form

This document is required for all client accounts and must be available prior to approval of any transaction. To ensure the accuracy of the information, the firm requires the client to sign and date the New Account Form.

Client Disclosure Forms

A client disclosure form ("Disclosure Form") may be required for specific situations as determined by the firm. A Disclosure Form provides the client with important risk disclosures and timely information that should be considered by the client before investing. A Disclosure Form also may require the client to provide the firm with additional suitability information to assist review and approval of the transaction.

Written Suitability Analysis from Registered Person

Whenever a transaction raises suitability concerns, the EVPA (or his or her superior) may require the Registered Person to provide a written explanation of the factors considered as a basis for the investment recommendation to the client. This writing may include additional client information regarding other financial resources and/or investment objectives not previously documented, and/or any other information deemed relevant by the firm.

Client Representation Letters

The firm may require the client to confirm important information provided by the client, and then relied on by the firm to determine the suitability of the transaction ("Client Representation Letter"). The firm also may require the client to confirm their understanding of the associated risks of the specific transaction under review. The Client Representation Letter does not eliminate the responsibility of the EVPA to review and approve the transaction.

Other Documentation

The firm may rely on other forms of documentation to evidence the suitability process when reviewing and approving transactions. Telephonic or written communications with the Registered Person, client, and/or other interested parties, and/or internal memoranda may be used to document the suitability process. For example, forms of other documentation may include a copy of the client's income tax returns, investment account statements and other means to verify financial assets held by the client, or a memo or notes written by the EVPA.

8.40 Hierarchy of Transaction Review and Approval

The established hierarchy of transaction review, and levels of authority involving the disposition of a transaction, is described below.

Registered Person

The Registered Person is accountable for establishing that the client is qualified for the transaction and for obtaining adequate suitability information from the client that he or she believes can be relied on as a basis for making an investment recommendation.

EVPA

The designated EVPA adheres to the firm's written supervisory control procedures to conduct a review of the merits of the proposed transaction introduced by the Registered Person. If the EVPA approves (endorses) the transaction it is then accepted by the firm and processed.

Evidence of the client's suitability determination is maintained with the transactional information. To evidence review and approval of the transaction, the EVPAs initials (or designee) are required for each transaction. All documents associated with a transaction are maintained together, under the supervision of the COO (or designee).

Suitability of Recommendations

The firm and its associated persons are required to adhere to the Rules of Fair Practice, when recommending to an investor the purchase, sale, or exchange of a DPP security, to have reasonable grounds to believe the recommendation is suitable for the customer based on the customer's investment objectives, other investments, financial situation and needs, tax status, and any other information known by the member or associated person. Additionally, the firm and associated person must determine that the investor has the appropriate investment objectives, is in a position to fully understand the risks and benefits of the transaction, and has a net worth sufficient to sustain the risks involved in an investment in a DPP security. While the firm believes that imposing a "one size fits all" methodology is impractical given the myriad of investor profiles, financial strengths, liquidity needs and risk tolerances; the firm relies on the EVPA to make reasonable efforts to obtain the customer information necessary to make the suitability determination.

In addition, the firm must consider the suitability standards that may be imposed by state law when making a finding of customer suitability. Prior to admitting a new limited partner, the firm requires new investors to obtain consent from the California Department of Corporations ("DOC"). Potential buyers provide suitability information to the DOC as an additional suitability review prior to admission into any new fund.

The requirement to make a suitability determination not only applies to any initial purchase of partnership securities but to secondary market transactions as well. In making recommendations, one must also be aware of their fundamental responsibility of fair dealing with customers including determining whether a reasonable basis exists for engaging in the DPP transaction, considering any tax implications to the customer, and the fairness of the recommended price for the purchase or sale.

The EVPA has authority at any time to contact the Registered Person on any issue of concern and/or request additional suitability documentation, to contact the client or other relevant individual and/or to refer a specific transaction to the next level of management for guidance.

EVPA Supervisor

Whenever the EVPA determines he or she cannot approve a transaction, he or she will have the CCO review the transaction. The CCO shall attempt to address the EVPA's issues of concerns such as procedural questions, measuring the adequacy of the suitability documentation for the transaction, or communication problems with the Registered Person.

If the concerns cannot be satisfactorily addressed, the CCO may seek assistance from the CEO and/or DSI's General Counsel to reconcile unresolved suitability issues or support possible corrective actions.

Generally, direct communication with the Registered Person by the CCO, CEO, and/or DSI's General Counsel will resolve the concerns or clearly establish the corrective action to be taken by the firm. After the steps listed above are taken, the principals make a final determination. If the final decision is that the transaction will not be approved, the business is returned to the Registered Person.

Compliance Oversight

The firm's surveillance function assists in determining if suitability concerns are a reoccurring event for a Registered Person and/or Branch Office. Any issues are incorporated into the on-going surveillance function.

Recordkeeping

The CCO ensures that the EVPA documents the review and approval of transactions.

8.50 Limited Size & Resources Exception

On July 31, 2009, DSI filed for the limited size and resources exception pursuant to Rule 3012. This filing became necessary given the limited size and scope of our broker/dealer. We will continue to rely on this exception and file annually, no later than the anniversary date, or until our business model warrants a change.

Chapter Nine

9.00 Client Account Activity

9.10 Transmittal of Client Funds or Securities

Processing the receipt of client checks and/or DSI Realty certificates received is considered an extremely critical procedure which must be performed in a timely manner (this generally means within 24 hours).

Requirements

Each DSI representative is required to maintain a listing of all checks received from customers and forwarded for securities transactions. The log should indicate the date when received, client name or account number, amount, destination, and how sent. If checks are not processed on the same day, they are locked and secured overnight. All client checks and/or certificates must be accompanied by a transmittal form and forwarded to the Home Office to be processed and posted to the records.

Review and Approval

Checks received at the Home Office are recorded in the 2159 Check Blotter and deposited the same day. The 2159 blotter is reviewed by the COO weekly as part of the Firm's Reserve Requirement Computation. Furthermore, deposits are reviewed and approved daily and also reconciled against bank statements at each month-end. Reviews and approvals of these items are evidenced by initials of the reviewing parties.

Recordkeeping

The COO supervises the process of transmittal of client funds or securities. Records of all transmittals and deposits are maintained in the home office.

Transmittals to Outside Entities

The firm permits transmittal of customer funds or securities to an outside entity or an address other than the primary address of the client, only if the address does not belong to the representative and the account holder signs a written request and submits it to the Home Office. If the request appears to be in good order, it will be processed accordingly.

9.15 Disclosure of Customer Fees

Pursuant to Rule 2420, charges, if any, for services performed, including miscellaneous services such as collection of moneys due for principal, dividends, or interest; exchange or transfer of securities; appraisals, safe-keeping or custody of securities, and other services, shall be reasonable and not unfairly discriminatory between customers.

Currently, the firm does not impose ANY fees for its services outside the commissions generated for resale transactions. This resale commission is disclosed to the client prior to execution.

9.20 Approval of Changes in Account Name/Designation

The DAS (or designee) has authority to approve any changes in account names or designations, provided the request is submitted in writing and signed by the client. This written approval process requires the documentation of the essential facts relied upon in approving the changes, which is maintained with the related new account information on file for the existing account holder.

9.30 Disclosure of Financial Condition to Customers

In accordance with FINRA Conduct Rule 2270, the firm makes available for inspection by any bona fide customer (defined in the Rule as someone for whom the firm holds cash or securities), upon request, the information relative to the firm's financial condition as disclosed in its most recent balance sheet prepared either in accordance with the firm's usual practice or as required by any state or federal securities regulation. Any such requests are handled by the COO (or designee).

9.40 Periodic Customer Account Review

The Compliance Staff conducts periodic reviews of customer accounts as part of the branch office inspection program to detect and prevent irregularities or abuses. Questionable activities are brought to the attention of the CCO.

9.50 Signature Guarantee Requirements

The firm is not a member of the Securities Transfer Agents Medallion Program (STAMP). Rather, the firm relies upon the HBI Securities Transfer Association Medallion Program (STAMP) Medallion Signature Guarantee Program, or the Medallion Signature Guarantee Program.

This is a controlled program under which HBI issues a Medallion signature guarantee stamp privileges to qualified authorized Registered Persons which allows them to provide Medallion signature guarantees on securities documents.

As a general policy, a Registered Person will not be considered for the Medallion Signature Guarantee Program until he or she has been affiliated with HBI and has submitted securities business to HBI for at least 90 calendar days. The 90-day waiting period may be waived by the HBI on a case by case basis.

HBI's assigned Compliance Staff maintains a record of all authorized persons issued a Medallion Stamp. The records include the original Request for Medallion Signature Guarantee Stamp, name of person assigned the Medallion Stamp, the Medallion Stamp number, the date of issuance, and date of return.

Additional Procedures

The procedures for using a Medallion Stamp and other related matters are set forth in the HBI Medallion Signature Guarantee Program Procedures distributed to the authorized persons upon acceptance into the Program.

Chapter Ten

10.00 Customer Complaint Management

10.10 Definition of Customer Complaint

A customer complaint is defined as any written or verbal statement made by a customer (or authorized person acting on behalf of such customer) directed against the firm and/or a Registered Person alleging a complaint involving securities or related activities in connection with the solicitation or execution of any transaction or the disposition of securities or funds of a customer.

The customer complaint process described below does not apply to clerical and administrative errors. The CCO (or designee), reviews and evaluates the specific circumstances to determine if a possible customer service problem involving clerical or administrative errors warrants classification as a customer complaint.

10.20 Notification of a Customer Complaint

Customer complaints are usually identified by one of the following means:

- Receipt of a written customer complaint
- Direct communication with a Supervisor or Registered Person
- Verbal communications with an investor
- Letter from a law firm presenting an investor
- Formal communications from the SEC, FINRA or other SRO
- Formal communications from a state securities agency as a result of a branch office inspection, inquiry, customer complaint, request for information, etc.
- Communications from other concerned parties such as an insurance company, investment company, etc.
- Documents connected to a legal proceeding, arbitration, etc.
- Branch Office inspection by the firm

Any Registered Person, Supervisor or firm employee who learns of a customer complaint must immediately report the matter to the CCO (or designee) for appropriate action. The failure by a Registered Person to make a timely report to the firm or attempts to make a private settlement of a customer complaint matter may have negative consequences for Errors and Omission Insurance coverage and result in additional enforcement action being taken by the firm and/or FINRA.

Current and Historical Records

Both current and historical customer complaints information is maintained by the assigned Compliance Staff. This data may be considered by the Home Office Principals when evaluating questionable practices or suitability determinations, or as part of the preparation of the Branch Office Inspection. When evaluating a current customer complaint, the history of any previous customer complaints involving the specific Registered Person is reviewed and considered.

10.30 Classification of Customer Complaint Matters

Any complaints received by DSI that relate to business that was conducted prior to its current approved business model/activity will be reported to the CCO immediately. The procedures for handling certain classifications of customer complaints are covered below.

Regulatory Inquiries

Regulatory inquiries are handled by the CCO in a manner similar to customer complaints.

FINRA Arbitration and Other Regulatory Action

FINRA arbitration claims and any other legal or regulatory proceeding are handled by the General Counsel, and any outside counsel designated by the firm, with the assistance and knowledge of the CEO, COO, CCO and other relevant parties.

10.40 Complaint Investigation Process

The Compliance Department has established the internal procedures described below for handling a customer complaint.

Complaint Files

For each customer complaint, the assigned Compliance Staff maintains an up-to-date, separately identifiable Complaint File. Complaint files are organized in chronological order and contain all related documentation and evidence of subsequent actions taken by the firm to analyze the records and circumstances connected with the allegations.

The assigned Compliance Staff maintains all customer complaint files in a centralized location in accordance with SEC Rule 17a-4.

Step-by-Step Process

When reviewing customer complaints, the CCO (or designee) takes the following actions:

1. Date stamps the complaint with the date of receipt.

2. Reviews the initial complaint information and any supporting documents provided by the investor, and/or other sources.

3. Sets up a Complaint File for the matter, and places the initial information and any information collected from the firm's records into the file.

4. Provides a written summary of the complaint matter for the file, and, if applicable, for the CCO and/or the COO.

5. Creates an internal record of the customer complaint for tracking and reporting purposes.

6. The firm will promptly acknowledge its receipt of the complaint with the customer.

7. Notifies the Registered Person of the complaint against them (if applicable) and establishes a deadline for providing additional information to the Compliance Department about the questioned transactions and/or activities.

8. Notifies the Registered Person's Supervisor of the ongoing complaint investigation, and, at the discretion of the CCO, asks the Supervisor to participate in the process as requested.

9. Assumes investigative control over the complaint matter, including collecting additional information from various sources to determine the merits of the complaint, verifying what events may have contributed to creating the complaint, and calculating any potential liability associated with the complaint.

10. If the matter has been assigned to staff, he or she provides the CCO with status reports about the progress of the investigation, and any other unresolved concerns and/or outstanding issues that need to be addressed.

11. Once the investigation has been completed and the matter is ready to be answered, the CCO determines whether to meet with the General Counsel to review the evidence. The CCO recommends and discusses a disposition.

12. The General Counsel confirms or modifies the recommended corrective action(s) prior to the CCO responding to the customer complaint.

13. Provides the Director of Licensing with a copy of the complaint and summary for timely reporting and disclosure to the CRD/FINRA with amendments to the Form U-4.

14. All customer complaints are reported by the CCO (or designee) in accordance with FINRA Conduct Rule 3070, as detailed below.

10.50 FINRA Conduct Rule 3070 Reporting Requirement

Material Event Reporting

Within 10 business days of discovery by the firm, the CCO (or designee) files notice with FINRA in the event any of the following conditions are applicable to either the firm or an Associated Person:

1. Has been found to have violated any provision of any securities law or regulation, any rule or standards of conduct of any governmental agency, self-regulatory organization, or financial business or professional organization, or engaged in conduct which is inconsistent with just and equitable principles of trade; and the member knows or should have known that any of the aforementioned events have occurred;

2. Is the subject of any written customer complaint involving allegations of theft or misappropriation of funds or securities or forgery;

3. Is named as a defendant or respondent in any proceeding brought by a regulatory or self-regulatory body alleging the violation of any provision of the Act, or of any other federal or state securities, insurance, or commodities statute, or of any rule or regulation hereunder, or of any provision of the By-laws, rules or similar governing instruments of any securities, insurance or commodities regulatory or self-regulatory organization;

4. Is denied registration or is expelled, enjoined, directed to cease and desist, suspended or otherwise disciplined by any securities, insurance or commodities industry regulatory or self-regulatory organization or is denied membership or continued membership in any such self-regulatory organization; or is barred from becoming associated with any member of any such self-regulatory organization;

5. Is indicted, or convicted of, or pleads guilty to, or pleads no contest to, any felony; or any misdemeanor that involves the purchase or sale of any security, the taking of a false oath, the making of a false report, bribery, perjury, burglary, larceny, theft, robbery, extortion, forgery, counterfeiting, fraudulent concealment, embezzlement, fraudulent conversion, or misappropriation of funds, or securities, or a conspiracy to commit any of these offenses, or substantially equivalent activity in a domestic, military, or foreign court;

6. Is a director, controlling stockholder, partner, officer or sole proprietor of, or an associated person with, a broker, dealer, investment company, investment advisor, underwriter or insurance company which was suspended, expelled or had its registration denied or revoked by any agency, jurisdiction or organization or is associated in such a capacity with a bank, trust company or other financial institution which was convicted of or pleaded no contest to, any felony or misdemeanor;

7. Is a defendant or respondent in any securities or commodities-related civil litigation or arbitration which has been disposed of by judgment, award or settlement for an amount exceeding $15,000. However, when the member is the defendant or respondent, then the reporting to the Association shall be required only when such judgment, award, or settlement is for an amount exceeding $25,000;

8. Is the subject of any claim for damages by a customer, broker, or dealer which is settled for an amount exceeding $15,000. However, when the claim for damages is against a member, then the reporting to the Association shall be required only when such claim is settled for an amount exceeding $25,000;

9. Is associated in any business or financial activity with any person who is subject to a “statutory disqualification” as that term is defined in the Act, and the member knows or should have known of the association. The report shall include the name of the person subject to the statutory disqualification and details concerning the disqualification; and/or

10. Is the subject of any disciplinary action taken by the member against any person associated with the member involving suspension, termination, the withholding of commissions or imposition of fines in excess of $2,500, or otherwise disciplined in any manner which would have significant limitation on the individual's activities on a temporary or permanent basis.

Customer Complaint Reporting

No later than 15 days of the month following the calendar quarter in which the customer complaint was received by the firm, to the extent required by FINRA Rule 3070 the CCO (or designee) files notice of the customer complaint with FINRA.

The reporting requirements of *Rule 3070 require the firm to promptly file with FINRA copies of:*

1. Any indictment, information or other criminal complaint or plea agreement for conduct reportable under paragraph (a)(5) of Rule 3070;

2. Any complaint in which a member is named as a defendant or respondent in any securities or commodities-related private civil litigation;

3. Any securities related arbitration claim filed against a member in any forum other than the FINRA Dispute Resolution forum;

4. Any indictment, information or other criminal complaint, any plea agreement, or any private civil complaint or arbitration claim against a person associated with a member that is reportable under question 14 on Form U-4, irrespective of any dollar thresholds Form U-4 imposes for notification, unless, in the case of an arbitration claim, the claim has been filed in the FINRA Dispute Resolution forum.

10.60 Action Resulting in Form BD and/or Form U-4 Amendment

The CCO (or designee) with the assistance of the Director of Licensing ensures that Form BD and/or Form U-4 is amended, if necessary, in connection with the resolution of a customer complaint or further escalation of such a matter.

Chapter Eleven

11.00 Patriot Act Procedures

11.10 Financial Crime Center (FinCEN)

Pursuant to Treasury Regulations, the firm responds to the Financial Crime Network ("FinCEN") requests about accounts or transactions by reporting to FinCEN the identity of the specified individual or organization, the account number, all identifying information provided by the account holder when the account was established, and the date and type of transaction.

If a match is confirmed by the firm, the information is reported directly on the FinCEN site and the AML Officer is immediately notified for consideration and appropriate follow-up actions.

EVIDENCE OF FINCEN REVIEWS

The EVPA or designee will evidence his or her review of account records in response to requests from FinCEN by printing the self-verification confirmation from their website.

11.20 AML Program

Money laundering is the process by which individuals attempt to conceal the true origin and ownership of the proceeds of illegal activities. Any involvement in a transaction that seeks to conceal or disguise the *nature, location, source, ownership* or *control* of proceeds derived from a wide range of crimes may constitute money laundering. It is especially important to note that the knowing receipt of the proceeds of illegal activity can constitute money laundering.

Federal laws, SEC and FINRA Rules mandate that DSI design, maintain, and enforce an AML program. Each Registered Person, because of the close personal contact with the investing public, is an integral part of the firm's AML controls, and has a duty to report possible suspicious client activity to the firm's AML Officer(s).

AML Program

The firm maintains a separate written DSI Anti-Money Laundering/Anti-Terrorism Compliance Program ("AML Program") which is attached to this Manual as Exhibit 2.

AML Officer

The firm has designated Kenneth A. Caleb, Vice President & COO as its AML Officer.

Recordkeeping

The COO and EVPA maintain the firm's AML records, including the annual review records.

Chapter Twelve

12.00 Financial Accounting & Reporting

12.10 Designation of Financial & Operations Principal

The firm has designated the Financial Principal "FINOP" as the person responsible for overseeing posting and maintaining all accounting, commission and financial information, reporting financial information, and exercising accounting controls in accordance with SEC Rule requirements and industry standards. These duties include calculating the firm's net capital requirements, maintaining existing safeguards to ensure compliance with the customer reserve requirement, and filing the firm's annual audit report and quarterly FOCUS IIA Reports.

The FINOP is qualified as a Financial & Operations Principal (Series 27).

12.20 Internal Accounting Records

The Accounting Department maintains the following books and records for the firm.

General Ledger

The General Ledger contains each account maintained by the firm. It is posted on a monthly basis by the General Ledger Analyst from other accounting records maintained by the firm. The firm's internal guideline is to complete the posting to the General Ledger by the 17th business day of each month.

Once all entries to the General Ledger have been entered and reconciled, a trial balance is printed reflecting the ending balances for each account at month end. The FINOP (or designee) reviews the trial balance to identify questionable fluctuations in account balances and researches any unusual or significant changes. If required, adjusting journal entries are made with supporting documentation. A month-end financial statement is then generated from the trial balances and reviewed by the FINOP.
All paperwork regarding the General Ledger is kept in a file, by month, in the General Ledger Analyst's office.

The Firm's Checking Accounts

The Accounting Department maintains the firm's checking accounts. Checkbooks are kept in a locked area. All checks written are approved by an authorized principal of the firm, who evidences his or her approval by initialing the check request or invoice. Two authorized signatures are required for every check issued by the firm. Monthly checking account statements are received by the firm directly from the bank.

Records, including voided checks, are reconciled and maintained by the COO under the direction and supervision of the FINOP.

Commission Records

The Accounting Department maintains the accounting for commission and fee revenues, and the subsequent payment to each Registered Person. These records are reconciled on a monthly basis and reported to the COO.

Prohibitions

Pursuant to NASD Rule 2420, commission payments are restricted to FINRA member broker-dealers and their registered agents.

12.30 Net Capital Requirement

In accordance with SEC Rule 15c3-1, the firm must maintain adequate net capital in order to conduct the firm's securities operations. The FINOP (or designee) is responsible for calculating the firm's net capital requirement on a monthly basis.

On the 17th day of each month, FINOP (or designee) generates the Net Capital Calculation for the firm along with the firm's monthly financial statements. The minimum net capital requirement is reviewed and compared to the prior month to identify any significant transactions and their impact on the current net capital requirement. The COO evidences the review by initialing and dating the first page of the monthly financial statement. The monthly financial statement and net capital calculation are then provided to the FINOP for final review and approval.

These records are maintained by, or under the direction and supervision of, the FINOP.

Early Warning Procedure:

If the firm's computed capital falls below 120% of its minimum requirement as a $250,000 broker/dealer, all of the the following shall take place immediately upon discovery:

1. The firm will immediately cease any broker/dealer functions until the net capital issue is resolved.

2. The FINOP (or designee) will immediately contact both FINRA and the SEC telephonically to provide notice that the firm has fallen into early warning.

3. The FINOP (or designee) will draft letters of explanation, which will also contain the current computation. These will be faxed or submitted electronically to both FINRA and the SEC within 24 hours of discovery.

12.40 Customer Reserve Rule

In accordance with SEC Rule 15c3-3, the firm operates pursuant to the exemption provisions of paragraph (k)(1)(iii) as an introducing broker/dealer and promptly transmits all customer funds and delivers all customer securities received in connection with securities activities, and does not otherwise hold funds or securities for, or owe money or securities to customers.

The firm also maintains a Special Bank Account Exclusively for the Benefit of Customers in accordance to the requirements of SEC Rule 15c3-3(e). Timely deposit of customer checks is made by no later than noon of the next business day. The FINOP (or designee) supervises activity subject to SEC Rule 15c3-3.

The FINOP (or designee) maintains these records and the required supporting documentation, including the bank notification letter required by SEC Rule 15c3-3 (f).

12.50 Financial Reporting

FOCUS, Part II A Report

In accordance with SEC Rule 17a-5, the firm is required to electronically file with FINRA on a quarterly basis, FOCUS Part II A Report. The FOCUS Part II A Report is filed by the FINOP (or designee) no later than the 17th business day following the previous quarter end. The COO provides copies of the filing and support documentation to the FINOP.

These records are maintained by, or under the direction and supervision of, the FINOP.

Annual Audit Report

In accordance with SEC Rule 17a-5, the firm is required to file on an annual basis audited financial statements within 60 days of the firm's fiscal year-end. The firm's Audit Report is provided to the SEC, FINRA, and regulatory authorities in various states in which the firm conducts business. The FINOP manages the relationship with the accounting firm selected by the firm to conduct the financial audit, and coordinates their review of books and records, staff interviews, and other requested documentation associated with the audit process. These records are maintained by, or under the direction and supervision of, the FINOP.

Chapter Thirteen

13.00 Marketing Activity

13.10 Due Diligence

The firm's due diligence review ("Due Diligence") is the formal process for exercising "reasonable care" in verifying the accuracy and completeness of statements made by a sponsor company. Due Diligence also includes the ongoing review of the various companies the firm maintains a business relationship with, and reporting any significant developments to senior management.

Primary investment products subject to the formal due diligence process include, and are currently limited to:

- Direct Participation Programs (public and private);
- Private Placements Offerings;

Due Diligence Review Process

Due Diligence is assigned to the EVPA, Due Diligence is supervised by the CCO.

Due Diligence includes the gathering of available information and verification, assessment and evaluation, recommendation and findings. Due Diligence tasks include:

1. Review of the prospectus or private offering memorandum to determine adequate disclosures.
2. Review of the previous two years of financial statements of the general partner and/or sponsor company.
3. Review of assumptions made for any financial models.
4. Assessment of the overall industry outlook.
5. Assessment of the qualifications of the business organization and key personnel.
6. Assessment of financial risks with special attention paid to the tax implications, appreciation of assets, projected rates of return, assets already in the portfolio, and general risks/benefit for investors.
7. Fairness of the partnership agreement, if applicable.
8. Review of the key business relationships of the general partner and/or sponsor company, including banks, attorneys, accountants, broker-dealers and other important vendors.
9. Review and assessment of past partnerships and investment results.
10. Review and evaluation of reported conflicts of interest.
11. Review and assessment of any other available relevant information.

Recordkeeping

The EVPA (or designee) maintains the Due Diligence records, including the sponsor files. The files for disapproved programs are maintained for at least one year.

13.20 New Product Review

As a general policy, the firm is not seeking to add new products to the traditional products and services currently offered.

The firm does not consider new enhancements or features applied to existing investment products, or the creation of a new alternative to the existing investment, as a "new product."

Preliminary Review

The firm's Due Diligence would conduct the preliminary evaluation of any types of new DPP offerings to be sold by the firm. Additional staff may be designated to assist with the collection and evaluation of information.

Due Diligence Review

If the CEO judges there is merit in further review of a new DPP offering, he will direct the EVP of Administration, Due Diligence to conduct a formal due diligence review.

Evaluation Review

After completion of the Due Diligence review, the COO, CCO and/or General Counsel, and possibly other selected managers, would consider and evaluate the business prospects of a new offering, such as profitability and demand, and the associated risks to the firm. Consideration would be given to the types of possible client disclosure documents and/or other limits that may need to be put in place prior to offering a new product to clients.

Final Determination

The CEO would be consulted prior to a final determination to offer any new DSI program.

Chapter Fourteen

14.00 Other Controls

14.10 Business Continuity Plan

Following the tragic events of September 11, 2001, pursuant to NTM 02-23, FINRA requested that broker-dealers create and maintain business continuity plans. The firm's first Business Continuity Plan (BCP) was created in light of FINRA Conduct Rule 3510 and NTM 04-37.

Updates and Annual Review

The firm's BCP will be updated as necessary to reflect any material change related to the firm's operations, structure, business or location, or that of its clearing firm(s). The BCP is reviewed during the 3rd quarter of each calendar year. DSI's BCP is also available on the Firm's website.

Senior Management Approval

The firm's principals review the current BCP and submit it for final approval of the CEO. The CEO must approve it as reasonably designed to enable the firm to meet its obligations to customers in the event of a significant business disruption, as defined in the BCP.

Recordkeeping

The COO (or designee) maintains the BCP records, except for the records regarding the annual review which are maintained by the assigned Compliance Staff.

14.20 Customer Information and Data Safeguarding

As stated in the Firm's Privacy Policy, we maintain physical, electronic and procedural safeguards to protect personal information. Customer data in files and on our computer systems are highly sensitive and shall be maintained by responsible persons in accordance with our risk-based technological procedures.

In today's electronic world the threat of identity theft is more prevalent than ever. It is our duty to protect the client information we have been entrusted with. All employees with access to such information shall be required to adhere to the Firm's policies and procedures and to participate in frequent training sessions regarding this important matter.

Sensitive customer data is housed centrally on our primary server which is password protected and locked during non-business hours. Access to this server is limited by network permissions and passwords which are maintained by the Director of Information Technology and the Chief Information Technology Officer. The server is closed to the outside world via physical firewalls preventing access outside of the home office. Furthermore, DSI's employees are required to log-off computers when not in use and shut them down completely at the end of each workday to further safeguard this sensitive data. All systems are audited frequently to assure that current software updates are installed and effective.

Any physical documents containing client SSNs or other sensitive information are either kept under lock and key or shredded for proper disposal.

ACCESS TO CUSTOMER RECORDS

Access to the completed documents and customer files is restricted to: Only those employees who are required by their job function to access this information; Management, Legal and Compliance staff in cases where the information is requested to resolve a customer dispute; Management Legal and Compliance staff in cases where such information is requested by a regulatory agency; or Others as specifically permitted by management.

COLLECTION OF CUSTOMER INFORMATION

The firm collects and records customer information on certain types of forms that contain personal and financial data. Samples of these documents are available by contacting the EVPA or The CCO, but should also be maintained at every branch office of the firm.

SECURITY OF CLIENT INFORMATION

Client information is to remain confidential and representatives and employees are prohibited from disclosing it in contravention of the firm's privacy policies and procedures. Any representative or employee who is unsure of the terms of the firm's privacy policy should contact The CCO with any questions. Representatives and employees of the firm have a duty to safeguard client records in their possession and control from unauthorized access.

DISPOSAL OF CLIENT INFORMATION

Recent amendments to Regulation S-P refer to the proper disposal of consumer report information and records. Our policies and procedures require that we take reasonable measures to protect against unauthorized access to or use of any client information. In the event that we dispose of client information, we will shred documents containing any identifying information. When disposing of electronic files or communication, all identifiers will be erased. For the purpose of safe-guarding client information, all representatives and employees of the firm must follow these procedures when disposing of any documents containing a customer‘s name, address, phone number, social security number, or email address. Please note that this is not a comprehensive list; use caution with disposal of all client documents, regardless of content.

DISCLOSURE OF INFORMATION

The firm may disclose any information as directed by the customer, where necessary to the conduct of its business, or where disclosure is required by law. Information may be disclosed for audit or to law enforcement and regulatory agencies to aid in the prevention of fraud. The firm will not make any disclosures of information to other companies without the customer‘s consent and does not sell customer lists nor does it sell customer names to catalogue companies.

FORMER CUSTOMERS

Even if a customer is no longer with DSI, the firm privacy policy will continue to apply.

DISTRIBUTION OF PRIVACY PLEDGE TO EMPLOYEES

All employees will be required to review the firm's Privacy Policy and procedures upon joining the firm, and annually thereafter. Each employee is required to acknowledge receipt and understanding of firm's Privacy Policy.

NEW TECHNOLOGIES

Technological advancements and other changes in the workplace have raised concerns regarding the safeguarding of customer information. The following procedures must be followed regarding two recent technology developments: Wi-Fi is a generic term often used to refer to wireless connectivity to the Internet. Use of wireless connections are subject to the risk of unauthorized access by outside parties and the difficulty of ensuring the security of wireless connections to the Internet. Therefore, employees are prohibited from using Wi-Fi technology to access customer account information unless the information is encrypted, firewalls and similar defensive software is installed or the employee is working on the Firm‘s premises. The EVPA must pre-approve the use of Wi-Fi technology for the Firms‘s business. Remote access to corporate networks through VPNs or other technology is prohibited by the firm. Firewalls and other protections to avert intrusion including virus protection software are required on all computers with access to sensitive client information.

14.30 Annual Meetings

Annual Compliance Meeting

In accordance with NASD Rule 3010 (a)(7), the firm shall conduct an annual meeting to discuss compliance matters relevant to the activities of the representatives. This meeting is to be conducted either in person or telephonically by the CCO. Evidence of attendance shall be maintained by the CCO along with a summation of topics which were discussed.

14.40 Outsourcing Arrangements

The firm may contract with outside vendors to perform certain required functions. The following table includes information relating to these contracted services. The CCO is charged with overseeing these relationships and ensuring the establishment and maintenance of proper documentation of all agreements. The COO will ensure that all such contracts are properly considered in the context of net capital/AI calculations, when applicable.

The firm currently has no such relationships in place. All services are currently performed by in-house staff. Should we establish any relationships in the future the following required information would be provided herein:

Name of Vendor _____
Location of Vendor _____
Services Provided _____
Date of Contract _____
Comments_____

EXHIBIT 1

Diversified Securities, Inc.
Home Office Supervisory Principals

DSI designates Home Office Principals to carry out the supervisory responsibilities for the firm. The title and registration status of these Principals and the effective dates their duties were assumed are listed below. All Principals are based in the Home Office located in Long Beach, California.

ROBERT J. CONWAY - CRD 52861
Terminated Licenses on 8/24/13
Series: S-00/S-1/SS-27 GS, GP, FN
President & Chief Executive Officer 11/1965
Chief Financial Officer 11/1965
Chairman 11/1965

JOSEPH W. STOK - CRD 437061
Series S-00/S-1/S-15/S63/S4, GS, GP, SROP/CROP, FCOP/MP/MR/OP
Chief Compliance Officer (CCO) 11/1970
Director 11/1970
Senior Vice President 11/1984
Secretary 11/1984
BCP Secondary Contact 4/2004

RICHARD P. CONWAY - CRD 1764994
Series S-7/S-24/S-63/S-65, GS, GP
Executive Vice President, Administration (EVPA) 9/2011
Asst. to Secretary 4/2006
BCP Primary Contact 4/2004
Compliance Examiner 10/2007
Chief Information Technology Officer 12/2009
Operations Professional 12/23/11
Director 9/2011

KENNETH A. CALEB - CRD 2031701
Series S-7/S-24/S-63, GS, GP
Vice President 4/2008
Chief Operations Officer (COO) 4/2008
Chief AML Officer 9/2009
Compliance Examiner 10/2007
Director of Information Technology 12/2009
Operations Professional 12/23/11

MICHAEL S. CONWAY - CRD 3108375
Series S-7/S-24/S-63, GS, GP
Vice President 4/2008
Director of Account Services (DAS) 4/2008
Compliance Examiner 10/2007

EXHIBIT 2

Diversified Securities, Inc.

Anti-Money Laundering (AML) Program
Compliance and Supervisory Procedures

1. Diversified Securities, Inc. AML Policy

It is the policy of Diversified Securities, Inc. ("DSI") to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities.

What is Money Laundering?
Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes.

2. AML Compliance Officers Designation and Duties

Senior Management has implemented a "Captain Structure" to front-line manage the AML duties and to communicate effectively within relevant departments. The Captains will be trained in DSI's AML policies and procedures and will then be responsible for disseminating updated information to their departments, whether it be internal or regulatory. These individuals are qualified by experience, knowledge and training, and are all Registered Principals of the Firm. The duties of the AML Compliance Officers will include monitoring DSI's compliance with AML obligations, overseeing communication and training for employees. DSI has reviewed FINRA Rules 1021 and 1031 for any applicable registration requirements and have determined that DSI is properly registered. The AML Compliance Officers will also ensure that proper AML records are kept. When warranted, the AML Compliance Officers will ensure Suspicious Activity Reports (SAR-SFs) are filed.

DSI will provide FINRA with contact information for the AML Compliance Officers, including name, title, mailing address, e-mail address, telephone number and facsimile number. DSI will promptly notify FINRA of any change to this information.

3. Giving AML Information to Federal Law Enforcement Agencies and Other Financial Institutions

FinCEN Requests Under PATRIOT Act Section 314

Under Treasury's final regulations (published in the Federal Register on September 26, 2002), we will respond to a Financial Crimes Enforcement Network (FinCEN) request about accounts or transactions by immediately searching our records, at our head office or at one of our branches operating in the United States, to determine whether we maintain or have maintained any account for, or have engaged in any transaction with, each individual, entity, or organization named in FinCEN's request. Upon receiving an information request, we will designate the appropriate AML Compliance Officer to be the point of contact regarding the request and to receive similar requests in the future. Unless otherwise stated in FinCEN's

request, we are required to search current accounts, accounts maintained by a named suspect during the preceding 12 months, and transactions conducted by or on behalf of or with a named subject during the preceding six months. If we find a match, we will report it to FinCEN by completing FinCEN's subject information form. This form can be sent to FinCEN by electronic mail at sys314a@fincen.treas.gov, or by facsimile transmission to 703-905-3660. If the search parameters differ from those mentioned above (for example, if FinCEN requests longer periods of time or limits the search to a geographic location), we will limit our search accordingly.

If we search our records and do not uncover a matching account or transaction, then we will not reply to a 314(a) request.

We will not disclose the fact that FinCEN has requested or obtained information from us, except to the extent necessary to comply with the information request. We will maintain procedures to protect the security and confidentiality of requests from FinCEN, such as those established to satisfy the requirements of Section 501 of the Gramm-Leach-Bliley Act.

We will direct any questions we have about the request to the requesting Federal law enforcement agency as designated in the 314(a) request.

Unless otherwise stated in the information request, we will not be required to treat the information request as continuing in nature, and we will not be required to treat the request as a list for purposes of the customer identification and verification requirements. We will not use information provided to FinCEN for any purpose other than (1) to report to FinCEN as required under Section 314 of the PATRIOT Act; (2) to determine whether to establish or maintain an account, or to engage in a transaction; or (3) to assist DSI in complying with any requirement of Section 314 of the PATRIOT Act.

Sharing Information With Other Financial Institutions

We will share information about those suspected of terrorist financing and money laundering with other financial institutions for the purposes of identifying and reporting activities that may involve terrorist acts or money laundering activities and to determine whether to establish or maintain an account or engage in a transaction. We will file with FinCEN an initial notice before any sharing occurs and annual notices afterwards. We will use the notice form found at www.fincen.gov. Before we share information with another financial institution, we will take reasonable steps to verify that the other financial institution has submitted the requisite notice to FinCEN, either by obtaining confirmation from the financial institution or by consulting a list of such financial institutions that FinCEN will make available. We understand that this requirement applies even with respect to financial institutions *with whom we are affiliated*, and so we will obtain the requisite notices from affiliates and follow all required procedures.

We will employ strict procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information, including segregating it from DSI's other books and records.

In addition to sharing information with other financial institutions about possible terrorist financing and money laundering, we will also share information about particular suspicious transactions with our clearing broker for purposes of determining whether one of us will file a SAR-SF. In cases in which we file a SAR-SF for a transaction that has been handled both by us and by the clearing broker, we may share with the clearing broker a copy of the filed SAR-SF, unless it would be inappropriate to do so under the circumstances, such as where we filed a SAR-SF concerning the clearing broker or one of its employees.

4. Checking the Office of Foreign Assets Control ("OFAC") List

Before opening an account we will check to ensure that a customer does not appear on Treasury's OFAC "Specifically Designated Nationals and Blocked Persons" List by utilizing the automated search tool on http://www.instantofac.com, and is not from, or engaging in transactions with people or entities from, embargoed countries and regions listed on the OFAC Web Site. Evidence of this check against the

OFAC list is kept in the form of a screen print of the search results and initials of the party that performed the search. Because the OFAC Web Site is updated frequently, we consult the list on a regular basis and subscribe to receive updates when they occur. We access these lists through various software programs to ensure speed and accuracy. We will also review existing accounts against these lists when they are updated.

In the event that we determine a customer, or someone with or for whom the customer is transacting, is on the SDN List or is from or engaging in transactions with a person or entity located in an embargoed country or region, we will reject the transaction and/or block the customer's assets and file a blocked assets and/or rejected transaction form with OFAC. We will also call the OFAC Hotline at 1-800-540-6322.

5. Customer Identification and Verification

In addition to the information we must collect under FINRA Rules 2110 (Standards of Commercial Honor and Principles of Trade), 2310 (Recommendations to Customers - Suitability), and 3110 (Books and Records), and SEC Rules 17a-3(a)(9) (Beneficial Ownership regarding Cash and Margin Accounts) and 17a-3(a)(17) (Customer Accounts), we collect certain customer identification information from each customer who opens an account; utilize risk-based measures to verify the identity of each customer who opens an account; record customer identification information and the verification methods and results; provide notice to customers that we will seek identification information and compare customer identification information with government-provided lists of suspected terrorists.

a. Required Customer Information

Prior to opening an account, we will collect the following information for all accounts, if applicable, for any person, entity or organization who is opening a new account and whose name is on the account: the name; date of birth (for an individual); an address, which will be a residential or business street address (for an individual), an Army Post Office ("APO") or Fleet Post Office ("FPO") number, or residential or business street address of next of kin or another contact individual (for an individual who does not have a residential or business street address), or a principal place of business, local office or other physical location (for a person other than an individual); an identification number, which will be a taxpayer identification number (for U.S. persons) or one or more of the following: a taxpayer identification number, passport number and country of issuance, alien identification card number or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard (for non-U.S. persons). In the event that a customer has applied for, but has not received, a taxpayer identification number, we will require written verification from the agency that is processing the application to confirm that the application was filed before the customer opens the account and to obtain the taxpayer identification number within a reasonable period of time after the account is opened.

When opening an account for a foreign business or enterprise that does not have an identification number, we will request alternative government-issued documentation certifying the existence of the business or enterprise.

b. Customers Who Refuse To Provide Information

If a potential or existing customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, our firm will not open a new account and, after considering the risks involved, consider closing any existing account. In either case, our AML Compliance Officer will be notified so that we can determine whether we should report the situation to FinCEN (i.e., file a Form SAR-SF).

Verifying Information

Based on the risk, and to the extent reasonable and practicable, we will ensure that we have a reasonable belief that we know the true identity of our customers by using risk-based procedures to verify and document the accuracy of the information we get about our customers. In verifying customer identity, we will analyze any logical inconsistencies in the information we obtain.

We will verify customer identity through documentary evidence, non-documentary evidence, or both. We will use documents to verify customer identity when appropriate documents are available. In light of the increased instances of identity fraud, we will supplement the use of documentary evidence by using the non-documentary means described below whenever possible. We may also use such non-documentary means, after using documentary evidence, if we are still uncertain about whether we know the true identity of the customer. In analyzing the verification information, we will consider whether there is a logical consistency among the identifying information provided, such as the customer's name, street address, zip code, telephone number (if provided), date of birth, and social security number.

Appropriate documents for verifying the identity of customers include, but are not limited to, the following:

- For an individual, an unexpired government-issued identification evidencing nationality, residence, and bearing a photograph or similar safeguard, such as a driver's license or passport; and
- For a person other than an individual, documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement, or a trust instrument.

We understand that we are not required to take steps to determine whether the document that the customer has provided to us for identity verification has been validly issued and that we may rely on a government-issued identification as verification of a customer's identity. If, however, we note that the document shows some obvious form of fraud, we must consider that factor in determining whether we can form a reasonable belief that we know the customer's true identity.

We will use the following non-documentary methods of verifying identity:

- Contacting a customer;

- Checking references with other financial institutions

We will use non-documentary methods of verification in the following situations: (1) when the customer is unable to present an unexpired government-issued identification document with a photograph or other similar safeguard; (2) when DSI is unfamiliar with the documents the customer presents for identification verification; (3) when the customer and firm do not have face-to-face contact; and (4) when there are other circumstances that increase the risk that DSI will be unable to verify the true identity of the customer through documentary means.

We will verify the information within a reasonable time before or after the account is opened. Depending on the nature of the account and requested transactions, we may refuse to complete a transaction before we have verified the information, or in some instances when we need more time, we may, pending verification, restrict the types of transactions or dollar amount of transactions. If we find suspicious information that indicates possible money laundering or terrorist financing activity, we will, after internal consultation with DSI's AML Compliance Officers, file a SAR-SF in accordance with applicable law and regulation.

d. Lack of Verification

When we cannot form a reasonable belief that we know the true identity of a customer, we will do the following: (A) not open an account; (B) impose terms under which a customer may conduct transactions while we attempt to verify the customer's identity; (C) close an account after attempts to verify customer's identity fail; and (D) file a SAR-SF in accordance with applicable law and regulation.

e. Recordkeeping

We will keep records containing a description of any document that we relied on to verify a customer's identity, noting the type of document, any identification number contained in the document, the place of

issuance, and if any, the date of issuance and expiration date. With respect to non-documentary verification, we will retain documents that describe the methods and the results of any measures we took to verify the identity of a customer.

f. Comparison with Government Provided Lists of Terrorists and Other Criminals

From time to time, we may receive notice that a Federal government agency has issued a list of known or suspected terrorists. Within a reasonable period of time after an account is opened (or earlier, if required by another Federal law or regulation or Federal directive issued in connection with an applicable list), we will determine whether a customer appears on any such list of known or suspected terrorists or terrorist organizations issued by any Federal government agency and designated as such by Treasury in consultation with the Federal functional regulators. We will follow all Federal directives issued in connection with such lists.

We will continue to comply with Treasury's Office of Foreign Asset Control rules prohibiting transactions with certain foreign countries or their nationals.

g. Notice to Customers

Notice to customers that DSI is requesting information from them to verify their identities is required by Federal law. This notice is incorporated into DSI's Account Agreement which is provided as part of the FORM TB.

h. Reliance on Another Financial Institution for Identity Verification

We may, under the following circumstances, rely on the performance by another financial institution (including an affiliate) of some or all of the elements of our customer identification program with respect to any customer that is opening an account or has established an account or similar business relationship with the other financial institution to provide or engage in services, dealings, or other financial transactions:

- When such reliance is reasonable under the circumstances;
- When the other financial institution is subject to a rule implementing the anti-money laundering compliance program requirements of 31 U.S.C. 5318(h), and is regulated by a Federal functional regulator; and
- When the other financial institution has entered into a contract with our firm requiring it to certify annually to us that it has implemented its anti-money laundering program, and that it will perform (or its agent will perform) specified requirements of the customer identification program.

6. Foreign Correspondent Accounts and Foreign Shell Banks

Detecting and Closing Correspondent Accounts of Unregulated Foreign Shell Banks

Section 313 of the USA PATRIOT Act prohibits securities broker-dealers from maintaining correspondent accounts for foreign shell banks, and requires that they take reasonable steps to ensure that they are not providing banking services to foreign shell banks indirectly through correspondent accounts maintained for other foreign banks. A shell bank is a foreign bank with no physical presence in any jurisdiction. As a matter of policy DSI does not, and has never, established, maintained, administered, or managed correspondent accounts for unregulated foreign shell banks. DSI will detect correspondent accounts by strictly adhering to our CIP (described in Section 5).

b. Certifications

DSI does not have any foreign bank accounts that would be subject to certification. However, if DSI encounters a foreign bank as a prospective client, DSI will require completion of a certification issued by the Treasury. We will send the certification forms to our foreign bank account holders for completion, which requires them to certify that they are not shell banks and to provide ownership and agent information. We will re-certify when we believe that the information is no longer accurate and at least once every three years.

c. Recordkeeping for Foreign Correspondent Accounts

DSI does not have any foreign correspondent accounts. However, if DSI encounters a foreign correspondent account, DSI will keep records identifying the owners of foreign banks with U.S. correspondent accounts and the name and address of the U.S. agent for service of legal process for those banks.

d. Summons or Subpoena of Foreign Bank Records; Termination of Correspondent Relationships.

If DSI were to receive a written request from a federal law enforcement officer for information concerning correspondent accounts, we will provide that information to the requesting officer not later than 7 days after receipt of the request. We will close, within 10 days, any account for a bank that we learn from Treasury or the Department of Justice has failed to comply with a summons or has contested a summon. We will scrutinize any account activity during that 10-day period to ensure that any suspicious activity is appropriately reported and to ensure that no new positions are established in these accounts.

7. Private Banking Accounts/Foreign Officials

We do not open or maintain private banking accounts. DSI will detect and reject private banking accounts by strictly adhering to our CIP described in Section 5.

8. Monitoring Accounts For Suspicious Activity

We will manually monitor a sufficient amount of account activity to permit identification of patterns of unusual size, volume, pattern or type of transactions, geographic factors such as whether jurisdictions designated as “non-cooperative” are involved, or any of the “red flags” identified in Section 8. b. below. We will look at transactions, including trading and wire transfers, in the context of other account activity to determine if a transaction lacks financial sense or is suspicious because it is an unusual transaction or strategy for that customer. Each AML Compliance Officer will be responsible for this monitoring, will document when and how it is carried out, and will report suspicious activities to the appropriate authorities. Among the information we will use to determine whether to file a Form SAR-SF are exception reports that include transaction size, location, type, number, and nature of the activity. We will create employee guidelines with examples of suspicious money laundering activity and lists of high-risk clients whose accounts may warrant further scrutiny. Our AML Compliance Officers will conduct an appropriate investigation before a SAR is filed. Our monitoring of specific transactions includes reviewing all transactions on a daily basis in an effort to identify irregularities and suspicious activities.

Emergency Notification to the Government by Telephone

When conducting due diligence or opening an account, we will immediately call Federal law enforcement when necessary, and especially in these emergencies: a legal or beneficial account holder or person with whom the account holder is engaged in a transaction is listed on or located in a country or region listed on the OFAC list, an account is held by an entity that is owned or controlled by a person or entity listed on the OFAC list, a customer tries to use bribery, coercion, or similar means to open an account or carry out a suspicious activity, we have reason to believe the customer is trying to move illicit cash out of the government’s reach, or we have reason to believe the customer is about to use the funds to further an act of terrorism. We will first call the OFAC Hotline at 1-800-540-6322. The other contact numbers we will use are: Financial Institutions Hotline (1-866-556-3974), local U.S. Attorney’s Office (916) 445-9555, local FBI Office (310) 477-6565, and local SEC Office (323) 965-3998.

Red Flags

Red flags that signal possible money laundering or terrorist financing include, but are not limited to:

- The customer exhibits unusual concern about DSI's compliance with government reporting requirements and DSI's AML policies (particularly concerning his or her identity, type of business

and assets), or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspicious identification or business documents.

- The customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer's stated business or investment strategy.

- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.

- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.

- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.

- The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.

- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.

- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.

- The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash, or asks for exemptions from DSI's policies relating to the deposit of cash.

- The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the $10,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.

- For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.

- The customer is from, or has accounts in, a country identified as a non-cooperative country or territory by the FATF.

- The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity.

- The customer's account shows numerous currency or cashiers check transactions aggregating to significant sums.

- The customer's account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.

- The customer's account has wire transfers that have no apparent business purpose to or from a country identified as a money laundering risk or a bank secrecy haven.

- The customer's account indicates large or frequent wire transfers, immediately withdrawn by check or debit card without any apparent business purpose.

- The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.

- The customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer of the proceeds out of the account.

- The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.

- The customer requests that a transaction be processed to avoid DSI's normal documentation requirements.

- The customer, for no apparent reason or in conjunction with other red flags, engages in transactions involving certain types of securities, such as penny stocks, Regulation S stocks, and bearer bonds, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence to ensure the legitimacy of the customer's activity.)

- The customer's account shows an unexplained high level of account activity with very low levels of securities transactions.

- The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, for no apparent purpose.

- The customer's account has inflows of funds or other assets well beyond the known income or resources of the customer.

Responding to Red Flags and Suspicious Activity

When a member of DSI detects any red flag he or she will investigate further under the direction of the AML Compliance Officers. This may include gathering additional information internally or from third-party sources, contacting the government, freezing the account, or filing a Form SAR-SF.

9. Suspicious Transactions and BSA Reporting

Filing a Form SAR-SF

DSI will file Form SAR-SFs for any account activity (including deposits and transfers) conducted or attempted through our firm involving (or in the aggregate) $5,000 or more of funds or assets where we know, suspect, or have reason to suspect: 1) the transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation, 2) the transaction is designed, whether through structuring or otherwise, to evade the any requirements of the BSA regulations, 3) the transaction has no business or apparent lawful purpose or is not the sort in which the customer would normally be expected to engage, and we know, after examining the background, possible purpose of the transaction and other facts, of no reasonable explanation for the transaction, or 4) the transaction involves the use of DSI to facilitate criminal activity.

We will not base our decision on whether to file a SAR-SF solely on whether the transaction falls above a set threshold. We will file a SAR-SF and notify law enforcement of all transactions that raise an identifiable suspicion of criminal, terrorist, or corrupt activities. In high-risk situations, we will notify the government immediately (See Section 8 for contact numbers) and will file a SAR-SF with FinCEN. Securities law violations that are reported to the SEC or a Self-Regulatory Organization (SRO) may also be reported promptly to the local U.S. Attorney, as appropriate.

We will not file SAR-SFs to report violations of Federal securities laws or SRO rules by our employees or registered representatives that do not involve money laundering or terrorism, but we will report them to the SEC or SRO.

All SAR-SFs will be periodically reported to the Board of Directors and senior management, with a clear reminder of the need to maintain the confidentiality of the SAR-SF.

We will report suspicious transactions by completing a SAR-SF and we will collect and maintain supporting documentation as required by the BSA regulations. We will file a SAR-SF no later than 30 calendar days after the date of the initial detection of the facts that constitute a basis for filing a SAR-SF. If no suspect is identified on the date of initial detection, we may delay filing the SAR-SF for an additional 30 calendar days pending identification of a suspect, but in no case, will the reporting be delayed more than 60 calendar days after the date of initial detection.

We will retain copies of any SAR-SF filed and the original or business record equivalent of any supporting documentation for five years from the date of filing the SAR-SF. We will identify and maintain supporting documentation and make such information available to FinCEN, any other appropriate law enforcement agencies, or federal or state securities regulators, upon request.

We will not notify any person involved in the transaction that the transaction has been reported, except as permitted by the BSA regulations. We understand that anyone who is subpoenaed or required to disclose a SAR-SF or the information contained in the SAR-SF, except where disclosure is requested by FinCEN, the SEC, or another appropriate law enforcement or regulatory agency or an SRO registered with the SEC, will decline to produce to the SAR-SF or to provide any information that would disclose that a SAR-SF was prepared or filed. We will notify FinCEN of any such request and our response.

Currency Transaction Reports (CTR)

Our firm prohibits the receipt of currency as described in our Supervisory Procedures Manual.

Currency and Monetary Instrument Transportation Reports (CMIR)

Our firm prohibits the receipt of currency as described in our Supervisory Procedures Manual.

Foreign Bank and Financial Accounts Reports (FBAR)

DSI will file with FinCEN an FBAR for any financial accounts of more than $10,000 that we hold, or for which we have signature or other authority over, in a foreign country. We will use the FBAR Form at http://www.fincen.gov/f9022-1.pdf.

Transfers of $3,000 or More Under the Joint and Travel Rule

When DSI transfers funds of $3,000 or more, we will record on the transmittal order at least the following information: the name and address of the transmitter and recipient, the amount of the transmittal order, the identity of the recipient's financial institution, and the account number of the recipient. We will also verify the identity of transmitters and recipients who are not established customers of DSI (i.e., customers of DSI who have not previously maintained an account with us or for whom we have not obtained and maintained a file with the customer's name, address, taxpayer identification number, or, if none, alien identification number or passport number and country of issuance).

10. AML Record Keeping

SAR-SF Maintenance and Confidentiality

DSI will hold SAR-SFs and any supporting documentation confidential. We will not inform anyone outside of a law enforcement or regulatory agency or securities regulator about a SAR-SF. We will refuse any subpoena requests for SAR-SFs or SAR-SF information and immediately tell FinCEN of any such subpoena we receive. We will segregate SAR-SF filings and copies of supporting documentation from other firm books and records to avoid disclosing SAR-SF filings. Our AML Compliance Officers will handle all subpoenas or other requests for SAR-SFs. We will share information with our clearing broker about suspicious transactions in order to determine when a SAR-SF should be filed. As mentioned earlier, we may share with the clearing broker a copy of the filed SAR-SF – unless it would be

inappropriate to do so under the circumstances, such as where we file a SAR-SF concerning the clearing broker or its employees.

Responsibility for AML Records and SAR Filing

Our AML Compliance Officers will be responsible to ensure that AML records are maintained properly and that SARs are filed as required.

Records Required

As part of our AML program, our firm will create and maintain SAR-SFs, CTRs, CMIRs, FBARs, and relevant documentation on customer identity and verification *(See* Section 5 above) and funds transfers and transmittals as well as any records related to customers listed on the OFAC list. We will maintain SAR-SFs and their accompanying documentation for at least five years. We will keep other documents according to existing BSA and other record keeping requirements, including certain SEC rules that require six-year retention.

11. Bank Secrecy Act - Implementing Regulations 31 CFR 103

a. Monetary Instruments Recordkeeping ($3,000 to $10,000)

*The sale of monetary instruments such as bank checks or drafts, cashier's checks, money orders or traveler's checks are **NOT** allowed under our current business model. DSI has never participated in these types of transactions, but notes the requirements.*

b. Extensions of Credit

*Extension of credit are **NOT** allowed under our current business model. DSI has never participated in these types of transactions, but notes the requirements.*

c. Currency Transfer

DSI maintains a record of each advice, request, or instruction received or given regarding any transaction resulting in the transfer of currency or other monetary instruments, funds, checks, investment securities, or credit of more than $10,000 to or from any person, account, or place outside the United States. A record must also be maintained if the transaction is later canceled if the record is "normally made." (31 CFR 103.33(b))

d. Transfer of funds

DSI maintains a record of each advice, request, or instruction given to another financial institution or other person located within or without the United States, regarding a transaction intended to result in the transfer of funds, or of currency, other monetary instruments, checks, investment securities, or credit, of more than $10,000 to a person, account or place outside the United States. (31 CFR 103.33(c))

e. Records of Wire (Funds) Transfer

DSI collects and retains the information specified in Section 103.33(e) and (g) in connection with all wire (funds) transfers of $3,000 or more. The information to be collected and retained depends upon: (1) the type of financial institution, (2) its role in the wire transfer (originator, intermediary, or beneficiary), (3) the amount of the wire transfer, and (4) the relationship of the parties to the transaction with the financial institution.

11. Training Programs

We will develop ongoing employee training under the leadership of the AML Compliance Officers and senior management. Our training will occur on at least an annual basis. It will be based on our firm's size, its customer base, and its resources.

Our training will include, at a minimum: how to identify red flags and signs of money laundering that arise during the course of the employees' duties; what to do once the risk is identified; what employees' roles are in DSI's compliance efforts and how to perform them; DSI's record retention policy; and the disciplinary consequences (including civil and criminal penalties) for non-compliance with the PATRIOT Act.

We will develop training in our firm. Delivery of the training may include educational pamphlets, videos, intranet systems, in-person lectures, and explanatory memos. Currently our training program consists of informational meetings and discussions of potential AML issues and how to identify them.

We will review our operations to see if certain employees require specialized additional training. Our written procedures will be updated to reflect any such changes.

12. Updates to DSI's AML Program

Pursuant to FINRA Rule 3011(b) DSI is required to integrate new rules into its AML Program in a timely fashion. DSI subscribes to and receives e-mail notifications from both FinCEN and OFAC to keep abreast of updates that might require amendments to our policies. In addition, as a matter of procedure, DSI's AML Officers check both the FinCEN and OFAC websites, no less than quarterly, to ensure that no e-mail transmissions or rule changes have been overlooked.

13. Program to Test AML Program

Staffing

The testing of our AML program will be performed by Goodrich Baron & Goodyear, LLC, an independent third party. They are an independent certified accounting firm that audits DSI on an annual basis.

Evaluation and Reporting

After Goodrich Baron & Goodyear, LLC has completed the testing, their findings will be reported to senior management and to DSI's AML Compliance Officers. Any resulting recommendations will be incorporated accordingly.

14. Monitoring Employee Conduct and Accounts

We will subject employee accounts to the same AML procedures as customer accounts, under the supervision of the AML Compliance Officers. We will also review the AML performance of supervisors, as part of their annual performance review. The AML Compliance Officer's accounts will be reviewed by the firm's senior management.

15. Confidential Reporting of AML Non-Compliance

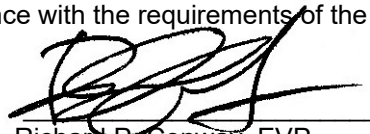
Employees will report any violations of DSI's AML compliance program to the AML Compliance Officers, unless the violations implicate the Compliance Officers, in which case the employee shall report to the President of the Firm. Such reports will be confidential, and the employee will suffer no retaliation for making them.

16. Additional Areas of Risk

DSI has reviewed all areas of its business to identify potential money laundering risks that may not be covered in the procedures described above. No additional areas of risk presently exist and therefore, no other procedures are necessary at this time.

17. Senior Manager Approval

I have approved this AML program as reasonably designed to achieve and monitor our firm's ongoing compliance with the requirements of the BSA and the implementing regulations under it.

Signed:  Date: November 18, 2015

By/Title: Richard P. Conway, EVP

EXHIBIT 3

Diversified Securities, Inc.

Business Continuity Plan

Emergency Contact Persons

Our firm's two emergency contact persons are: Richard P. Conway, (562) 493-8881, rickc@divsecs.com and Joseph W. Stok, (562) 493-8881, jstok@divsecs.com both of whom are Registered Principals of the firm. These names will be updated in the event of a material change.

Firm Policy

Diversified Securities, Inc. ("DSI") has implemented a business continuity plan ("BCP") in the event that a function deemed critical to DSI's ongoing business operations fails. The plan will assist DSI to eliminate and minimize any business interruptions as a result of an unexpected disaster. The plan has been tested at various times. Our firm's policy is to respond to a Significant Business Disruption (SBD) by safeguarding employees' lives and firm property, making a financial and operational assessment, quickly recovering and resuming operations, protecting all of the firm's books and records, and allowing our customers to transact business.

Significant Business Disruptions (SBDs)

Our plan anticipates two kinds of SBDs, internal and external. Internal SBDs affect only our firm's ability to communicate and do business, such as a fire in our building. External SBDs prevent the operation of the securities markets or a number of firms, such as a terrorist attack, a city flood, or a wide-scale, regional disruption.

Approval and Execution Authority

Richard P. Conway, EVPA, a registered principal, is responsible for approving the plan and for conducting the required annual review. Richard P. Conway, EVPA has the authority to execute this BCP.

Plan Location and Access

Our firm will maintain copies of its BCP plan and the annual reviews, and the changes that have been made to it for inspection. An electronic copy of our plan is located on our network server at our corporate headquarters in Long Beach.

Business Description

DSI is an introducing broker/dealer which has currently limited its business to servicing and maintaining limited partner clients within its DSI Realty Income DPPs. Consistent with its business continuity plan, DSI maintains back-up facilities in geographic locations separate from its primary facilities. Using these back-up facilities, DSI intends to continue its business in the event of a significant business disruption. Nevertheless, there are some disruptions that may render the firm unable to conduct business. Under such circumstances, DSI will ensure that clients will be able to access their account information within a reasonable time via either the internet or telephone.

Office Locations

Office Location #1 Corporate Headquarters & Branch Office

Our Main Office is located at 6700 E. Pacific Coast Hwy, Suite. #150, Long Beach, CA 90803. Its main telephone number is (562) 493-8881. Our employees may travel to that office by means of; foot, car, bus, cab, or boat.

Office Location #2 Tustin Office

Our Tustin Office is located at 17822 E. 17th St. #104, Tustin, CA 92780. Its main telephone number is (714) 547-0000. Our employees may travel to that office by means of; foot, car, bus, or cab.

Office Location #3 West Covina Office

Our West Covina Office is located at 1000 Lakes Dr., Suite #420, West Covina, CA 91790. Its main telephone number is (626) 919-3456. Our employees may travel to that office by means of; foot, car, bus, or cab.

Office Location #4 Visalia Office

Our Visalia Office is located at 2906 W. Main St. Visalia, CA 93278. Its main telephone number is (559) 732-3916. Our employees may travel to that office by means of; foot, car, bus, or cab.

Office Location #5 Covina Office

Our Covina Office is located at 861 S. Oak Park Road, 2nd Floor, Covina CA 91724. Its main telephone number is (626) 919-5223. Our employees may travel to that office by means of; foot, car, bus, or cab.

Alternative Physical Location(s) of Employees

In the event of an SBD, we will move our staff from affected offices to the closest of our unaffected office locations. If none of our other office locations is available to receive those staff, we have the ability to work remotely by accessing an archived version of the DSI Realty Income Fund software program from one of our offsite archive locations.

Customers' Access to Funds and Securities

DSI does not maintain custody of customers' funds or securities. In the event of an internal or external SBD, if telephone service is available, our limited partners will receive status updates by calling our emergency hotline at (800) 732-1733. If our Web access is available, our firm will post emergency notifications on our Web site. In addition, the firm will make this information available to customers through its disclosure policy.

SIPC Trustee Appointment

If SIPC determines that we are unable to meet our obligations to our customers or if our liabilities exceed our assets in violation of Securities Exchange Act Rule 15c3-1, SIPC may seek to appoint a trustee to disburse our assets to customers. We will assist SIPC and the trustee by providing our books and records identifying customer accounts subject to SIPC regulation.

Data Back-Up and Recovery (Hard Copy and Electronic)

Our firm maintains its primary hard copy and electronic books and records at our Corporate Headquarters located at 6700 E. Pacific Coast Highway, Suite #150, Long Beach, CA 90803. Our department managers are responsible for the maintenance of these books and records. This process is conducted and supervised by Richard P. Conway, our Executive Vice President of Administration. Please refer to the Emergency Contact Persons section above for his contact information.

In addition to duplicate records that are maintained at each of our Branch Locations, our firm maintains its archived hard copy books and duplicate electronic records at our offsite storage facility. This facility, Mini-U-Storage is located at 7611 Talbert Ave., Huntington Beach, CA.

DSI backs up its electronic records daily on several hard drives that are configured in a RAID array. In addition duplicate copies of electronic records are stored at the Mini-U-Storage facility in Huntington Beach.

In the event of an internal or external SBD that causes the loss of our paper records, we will physically recover them from our Branch locations. For the loss of our electronic records, we will physically recover the storage media from our back-up site.

Financial and Operational Assessments

Operational Risk

In the event of an SBD, we will immediately identify what means will permit us to communicate with our customers, employees, critical business constituents, critical banks, critical counter-parties, and regulators. Although the effects of an SBD will determine the means of alternative communication, the communications options we will employ will include our website at www.divsecs.com, our emergency telephone number (800) 732-1733, and our emergency email address: 911@divsecs.com. In addition, we will retrieve our key activity records as described in Section VII above, Data Back-Up and Recovery (Hard Copy and Electronic).

Financial and Credit Risk

In the event of an SBD, we will determine the value and liquidity of our investments and other assets to evaluate our ability to continue to fund our operations and remain in capital compliance. We will contact critical banks, and investors to apprise them of our financial status. If we determine that we may be unable to meet our obligations to those counter-parties or otherwise continue to fund our operations, we will request additional financing from our bank or other credit sources to fulfill our obligations to our customers and clients. If we cannot remedy a capital deficiency, we will file appropriate notices with our regulators and immediately take appropriate steps as necessary.

Mission Critical Systems

Our firm's "mission critical systems" are those that ensure prompt and accurate processing of our proprietary DPP transactions, including the maintenance of customer accounts, access to customer accounts, and the delivery of income distributions and certificates. These tasks are accomplished by utilizing our proprietary software program which was developed to perform these functions. This software system is the means by which we access all of our DSI Realty accounts.

Recovery-time objectives provide concrete goals to plan for and test against. They are not, however, hard and fast deadlines that must be met in every emergency situation, and various external factors surrounding a disruption, such as time of day, scope of disruption, and status of critical infrastructure—particularly telecommunications—can affect actual recovery times. Recovery refers to the restoration of clearing and settlement activities after a wide-scale disruption; resumption refers to the capacity to accept and process new transactions and payments after a wide-scale disruption. All DSI operational facilities are equipped for resumption of business and are tested several times per year. Our recovery time objective for our critical systems, including those involving a relocation of personnel or technology, is four (4) hours. This recovery objective may be negatively affected by the unavailability of external resources and circumstances beyond our control.

Alternate Communications Between the Firm and Customers, Employees, and Regulators

A. Customers

Currently, we communicate with our customers using the telephone, e-mail, our Web site, fax, U.S. mail, and in person visits at our firm or at the other's location. In the event of an SBD, we will assess which means of communication are still available to us, and use the means closest in speed and form (written or oral) to the means that we have used in the past to communicate with the other party. For example, if we have communicated with a party by e-mail but the Internet is unavailable, we will call them on the telephone and follow up where a record is needed with paper copy in the U.S. mail.

B. Employees

We now communicate with our employees using the telephone, e-mail, and in person. In the event of an SBD, we will assess which means of communication are still available to us, and use the means closest in speed and form (written or oral) to the means that we have used in the past to communicate with the other party. We will also employ a call tree so that senior management can reach all employees quickly during an SBD. The call tree includes all staff home and office phone numbers. We have identified persons, noted below, who live near each other and may reach each other in person:

The person to invoke use of the call tree is Richard P. Conway:

Caller	Call Recipients
Richard P. Conway	*Kenneth Caleb, Joseph W. Stok, Louisa Gac*
Kenneth Caleb	*Branch Locations*
Joseph W. Stok	*Kenneth Caleb, Michael Conway*
Louisa Gac	*Administrative Personnel*
Kenneth Caleb	*Operations Personnel*
Michael Conway	*Sales Personnel*

C. Regulators

We are currently members of the following SROs: The FINRA and SIPC. We communicate with our regulators using the telephone, e-mail, internet-based systems, fax, U.S. mail, and in person. In the event of an SBD, we will assess which means of

communication are still available to us, and use the means closest in speed and form (written or oral) to the means that we have used in the past to communicate with the other party.

Should you wish to contact any of our regulators directly, you may use the information provided below:

Regulator Contact Information:

FINRA
Los Angeles Regional Office
300 South Grand Avenue, Suite 1600
Los Angeles, CA 90071-3126
(213) 229-2300

Securities & Exchange Commission
Los Angeles Regional Office
5670 Wilshire Boulevard, 11th Floor
Los Angeles, CA 90036-3648
(323) 965-3998

CA Department of Corporations
320 West 4th Street, Suite 750
Los Angeles, CA 90013-2344
(213) 576-7500

Critical Business Constituents, Banks, and Counter-Parties

Business constituents

We have contacted our critical business constituents and have determined the extent to which we can continue our business relationship with them in light of the internal or external SBD. We will quickly establish alternative arrangements if a business constituent can no longer provide the needed goods or services when we need them because of a SBD to them or our firm.

Banks

We have contacted our bank to determine if they can continue to provide the operational capacities that we will need in light of the internal or external SBD. The bank maintaining our operating account is: Union Bank of California, 400 California Street, 9th Floor, San Francisco, CA 94104 (415) 765-2969. If our bank and other lenders are unable to provide the financing, we will seek alternative financing immediately via alternative recommendations from our existing banks.

Counter-Parties

We have contacted our critical counter-parties, such as other broker-dealers or institutional customers, to determine if we will be able to carry out our transactions with them in light of the internal or external SBD. Where the transactions cannot be completed, we will consult their Business Continuity procedures in order to make alternative arrangements to complete those transactions as soon as possible.

Regulatory Reporting

Our firm is subject to regulation by the SEC and the FINRA. We now file reports with our regulators using paper copies in the U.S. mail, and electronically using fax, e-mail, and the Internet. In the event of an SBD, we will check with the SEC, FINRA, and other regulators to determine which means of filing are still available to us, and use the means closest in speed and form (written or oral) to our previous filing method. In the event that we cannot contact our regulators, we will continue to file required reports using the communication means available to us.

Disclosure of Business Continuity Plan

We provide in writing a BCP disclosure statement to customers at account opening. We also post the disclosure statement on our Web site and mail it to customers upon request. Our disclosure statement is attached.

Updates and Annual Review

Our firm will update this plan whenever we have a material change to our operations, structure, business or location or to those of our clearing firm. In addition, our firm will review this BCP annually, on August 1st, to modify it for any changes in our operations, structure, business, or locations mentioned herein.

Senior Manager Approval

I have approved this Business Continuity Plan as reasonably designed to enable our firm to meet its obligations to customers in the event of an SBD.

Signed: _____

Richard P. Conway
Executive Vice President

Date: November 18, 2015

EXHIBIT 4

Diversified Securities, Inc.
DSI's Privacy Policy

DSI's Privacy Policy - A Commitment to Your Privacy

At Diversified Securities, Inc. ("DSI") our most important asset is our relationship with you. We are honored that you have entrusted us with your financial affairs, and we are committed to safeguarding the privacy of information we maintain about you. Establishing and adhering to an effective privacy policy is an important part of that dedication.

Below, you will find details about DSI's commitment to protecting your privacy, including the types of information we collect about you, how we use and share that information both within and outside the DSI family of companies, and how you can instruct us to limit certain types of information sharing.

Our privacy policy applies to all clients with whom we have a relationship and is also extended to each of our former clients.

Your Privacy Is Not for Sale

Simply put, we do not and will not sell your personal information to anyone, for any reason, at any time.

How We Collect Information About You

We collect personal information about you in a number of ways.

- Application and registration information.
  We collect information from you when you open an account. We may also collect information from consumer reporting agencies to verify your identity in the account-opening process or if you apply for a margin account. The information we collect may include your name, address, phone number, email address, Social Security number and date of birth, as well as details about your interests, investments and investment experience.
- Transaction and experience information.
  Once you have opened an account with us, we collect and maintain personal information about your account activity, including your transactions, balances, positions and history. This information allows us to administer your account and provide the services you have requested.
- Third-party information providers.
  We may collect information about you from information services and consumer reporting agencies to verify your identity, employment or creditworthiness, or to better understand your financial needs.

How We Share Information About You Within the DSI Family of Companies

Many clients within the DSI family of companies do business with more than one affiliate, creating an efficient, comprehensive financial relationship to meet individual needs. When appropriate, DSI may share information we collect about you within our family of companies to:

- help provide you with better service or perform services on our behalf;
- respond to communications from you or as you authorize or request;
- make it more convenient for you to open a new account;

You may instruct us **not** to share information about you with our affiliates for certain purposes, as explained under "How to Limit the Sharing of Information About You."

How We Share Information About You Outside of the DSI Family of Companies

We provide access to information about you to outside companies and other third parties in certain limited circumstances, including:

- to help us process transactions for your account;
- when we use another company to provide services for us, such as printing and mailing your account statements;
- when we believe that disclosure is required or permitted under law. For example, we may be required to disclose personal information to cooperate with regulatory or law enforcement authorities, to resolve consumer disputes, to perform credit/authentication checks, or for risk control;

You may instruct us **not** to share information about you with outside companies, as explained under "How to Limit the Sharing of Information About You."

How to Limit the Sharing of Information About You

If you prefer, you may choose to limit the information we share about you with our affiliates and outside companies. Specifically, you may instruct us:

- **not** to share with our affiliates consumer reports and other personal information about you that may be used to determine your eligibility for credit (for example, information about your income, profession, or employment status);
- You may exercise this choice by calling us at:
  562-493-8881; or **714-527-7789**
  from outside these area codes at: **800-732-1733**
- Joint account holders may instruct us on behalf of another account holder.
- You may make your privacy choice at any time and it will remain in effect until you change it.

If you choose to limit these types of information sharing, we may continue to share information with our affiliates that identifies you (such as your name and Social Security number), as well as information about your transactions and experiences with us. In addition, our affiliates may continue to use information they receive from us to perform services on our behalf, to respond to communications from you, as you authorize or request, or, if you are their customer, to offer you products or services. We may also continue to share information about you with outside companies as permitted or required by law.

State Laws

We will comply with state laws that apply to the disclosure or use of information about you.

Safeguarding Your Information, Maintaining Your Trust

We take precautions to ensure the information we collect about you is protected and is accessed only by authorized individuals or organizations.

Companies we use to provide support services are not allowed to use information about our clients for their own purposes and are contractually obligated to maintain strict confidentiality. We limit their use of information to the performance of the specific services we have requested.

We restrict access to personal information by our employees and agents. Our employees are trained about privacy and are required to safeguard personal information.

We maintain physical, electronic and procedural safeguards to protect personal information.

Teaming Up Against Identity Theft

Identity theft is a serious concern to all of us. Safeguarding information to help protect you from identity theft is our priority. DSI takes steps to protect you from identity theft by:

- utilizing client identification and authentication procedures before initiating transactions;
- creating a secure transmission connection to our DSI Websites. You will see the padlock in the lower right corner of your browser's frame indicating it is a secure site;
- ensuring our employees are trained to safeguard personal information about you.

You can also help protect your identity and accounts. Here are a few steps to remember:

- DSI will never request your account number, login password, or Social Security number in either a non-secure or unsolicited email communication;
- shred documents that contain personal information;
- check your credit report regularly for unauthorized activity and protect your personal identification numbers (PINs) or personal data.

Greater Accuracy Means Better Protection

We are committed to keeping accurate, up-to-date records to help ensure the integrity of the information we maintain about you. If you identify an inaccuracy in this information, or you need to make a change to it, please contact us promptly by calling **800-732-1733**.

A Commitment to Keeping You Informed

We will provide you with advance notice of important changes to our information-sharing practices.

Contact Us with Questions

In the event you have an emergency and/or complaint and are unable to reach your representative, you may contact our Compliance Department by email at dsiadmin@divsecs.com or call us at **800-732-1733**.

EXHIBIT 5

Diversified Securities, Inc.
Identity Theft Prevention Program (ITPP)
under the FTC FACT Act Red Flags Rule

Firm Policy

Our firm's policy is to protect our customers and their accounts from identity theft and to comply with the FTC's Red Flags Rule. We will do this by developing and implementing this written ITPP, which is appropriate to our size and complexity, as well as the nature and scope of our activities. This ITPP addresses 1) identifying relevant identity theft Red Flags for our firm, 2) detecting those Red Flags, 3) responding appropriately to any that are detected to prevent and mitigate identity theft, and 4) updating our ITPP periodically to reflect changes in risks.

Our identity theft policies, procedures and internal controls will be reviewed and updated periodically to ensure they account for changes both in regulations and in our business.

Rule: 16 C.F.R. § 681.1(d).

ITPP Approval and Administration

The firm's Chief Compliance Officer approved this initial ITPP. Kenneth A. Caleb, a member of senior management, is the designated identity theft officer and is responsible for the oversight, development, implementation and administration (including staff training and oversight of third party service providers of ITTP services) of this ITPP.

Rule: 16 C.F.R. § 681.1(e) and Appendix A, Section VI.(a).

Relationship to Other Firm Programs

We have reviewed other policies, procedures and plans required by regulations regarding the protection of our customer information, including our policies and procedures under Regulation S-P, [and] our CIP and red flags detection under our AML Compliance Program in the formulation of this ITPP, and modified either them or this ITPP to minimize inconsistencies and duplicative efforts.

Rule: 16 C.F.R. § 681.1, Appendix A, Section I.

Identifying Relevant Red Flags

To identify relevant identity theft Red Flags, our firm assessed these risk factors: 1) the types of covered accounts it offers, 2) the methods it provides to open or access these accounts, and 3) previous experience with identity theft. Our firm also considered the sources of Red Flags, including identity theft incidents our firm has experienced, changing identity theft techniques our firm thinks likely, and applicable supervisory guidance. In addition, we considered Red Flags from the following five categories (and the 26 numbered examples under them) from Supplement A to Appendix A of the FTC's Red Flags Rule, as they fit our situation: 1) alerts, notifications or warnings from a credit reporting agency; 2) suspicious documents; 3) suspicious personal identifying information; 4) suspicious account activity; and 5) notices from other sources. We understand that some of these categories and examples may not be relevant to our firm and some may be relevant only when combined or considered with

other indicators of identity theft. We also understand that the examples are not exhaustive or a mandatory checklist, but a way to help our firm think through relevant red flags in the context of our business. Based on this review of the risk factors, sources, and FTC examples of red flags, we have identified our firm's Red Flags, which are contained the first column ("Red Flag") of the attached "Red Flag Identification and Detection Grid" ("Grid").

Rule: 16 C.F.R. § 681.1(d)(2)(i) and Appendix A, Section II.

Detecting Red Flags

We have reviewed our covered accounts, how we open and maintain them, and how to detect Red Flags that may have occurred in them. Our detection of those Red Flags is based on our methods of getting information about applicants and verifying it under our CIP of our AML compliance procedures, authenticating customers who access the accounts, and monitoring transactions and change of address requests. For opening covered accounts, that can include getting identifying information about and verifying the identity of the person opening the account by using the firm's CIP. For existing covered accounts, it can include authenticating customers, monitoring transactions, and verifying the validity of changes of address. Based on this review, we have included in the second column ("Detecting the Red Flag") of the attached Grid how we will detect each of our firm's identified Red Flags.

Rule: 16 C.F.R. § 681.1(d)(2)(ii) and Appendix A, Section III.

Preventing and Mitigating Identity Theft

We have reviewed our covered accounts, how we open and allow access to them, and our previous experience with identity theft, as well as new methods of identity theft we have seen or foresee as likely. Based on this and our review of the FTC's identity theft rules and its suggested responses to mitigate identity theft, as well as other sources, we have developed our procedures below to respond to detected identity theft Red Flags.

Procedures to Prevent and Mitigate Identity Theft

When we have been notified of a Red Flag or our detection procedures show evidence of a Red Flag, we will take the steps outlined below, as appropriate to the type and seriousness of the threat:

Applicants. For Red Flags raised by someone applying for an account:

1. Review the application. We will review the applicant's information collected for our CIP under our AML Compliance Program (e.g., name, date of birth, address, and an identification number such as a Social Security Number or Taxpayer Identification Number).
2. Get government identification. If the applicant is applying in person, we will also check a current government-issued identification card, such as a driver's license or passport.
3. Seek additional verification. If the potential risk of identity theft indicated by the Red Flag is probable or large in impact, we may also verify the person's identity through non-documentary CIP methods, including:
    a. Contacting the customer
    b. Independently verifying the customer's information by comparing it with information from a credit reporting agency, public database or other source such as a data broker [or] the Social Security Number Death Master File.
    c. Checking references with other affiliated financial institutions, or
    d. Obtaining a financial statement.
4. Deny the application. If we find that the applicant is using an identity other than his or her own, we will deny the account.
5. Report. If we find that the applicant is using an identity other than his or her own, we will report it to appropriate local and state law enforcement; where organized or wide spread crime is suspected, the FBI or Secret Service; and if mail is involved, the US Postal Inspector. We may also, as recommended by FINRA's Customer Information Protection web page's "Firm Checklist for Compromised Accounts," report

it to our FINRA coordinator; the SEC; State regulatory authorities, such as the state securities commission; and our clearing firm.

6. Notification. If we determine personally identifiable information has been accessed, we will prepare any specific notice to customers or other required notice under state law.

Access seekers. For Red Flags raised by someone seeking to access an existing customer's account:

1. Watch. We will monitor, limit, or temporarily suspend activity in the account until the situation is resolved.
2. Check with the customer. We will contact the customer using our CIP information for them, describe what we have found and verify with them that there has been an attempt at identify theft.
3. Heightened risk. We will determine if there is a particular reason that makes it easier for an intruder to seek access, such as a customer's lost wallet, mail theft, a data security incident, or the customer's giving account information to an imposter pretending to represent the firm or to a fraudulent web site.
4. Check similar accounts. We will review similar accounts the firm has to see if there have been attempts to access them without authorization.
5. Collect incident information. For a serious threat of unauthorized account access we may, as recommended by FINRA's Customer Information Protection web page's "Firm Checklist for Compromised Accounts," collect if available:
    a. Firm information (both introducing and clearing firms):
        i. Firm name and CRD number
        ii. Firm contact name and telephone number
    b. Dates and times of activity
    c. Securities involved (name and symbol)
    d. Details of trades or unexecuted orders
    e. Details of any wire transfer activity
    f. Customer accounts affected by the activity, including name and account number, and
    g. Whether the customer will be reimbursed and by whom.
6. Report. If we find unauthorized account access, we will report it to appropriate local and state law enforcement; where organized or wide spread crime is suspected, the FBI or Secret Service; and if mail is involved, the US Postal Inspector. We may also, as recommended by FINRA's Customer Information Protection web page's "Firm Checklist for Compromised Accounts," report it to our FINRA coordinator; the SEC; State regulatory authorities, such as the state securities commission; and our clearing firm.
7. Notification. If we determine personally identifiable information has been accessed that results in a foreseeable risk for identity theft, we will prepare any specific notice to customers or other required under state law.
8. Review our insurance policy. Since insurance policies may require timely notice or prior consent for any settlement, we will review our insurance policy to ensure that our response to a data breach does not limit or eliminate our insurance coverage.
9. Assist the customer. We will work with our customers to minimize the impact of identity theft by taking the following actions, as applicable:
    a. Offering to change the password, security codes or other ways to access the threatened account;
    b. Offering to close the account;
    c. Offering to reopen the account with a new account number;
    d. Not collecting on the account or selling it to a debt collector; and
    e. Instructing the customer to go to the FTC Identity Theft Web Site to learn what steps to take to recover from identity theft, including filing a complaint using its online complaint form, calling the FTC's Identity Theft Hotline 1-877-ID-THEFT (438-4338), TTY 1-866-653-4261, or writing to Identity Theft Clearinghouse, FTC, 6000 Pennsylvania Avenue, NW, Washington, DC 20580.

Rule: 16 C.F.R. § 681.1(d)(iii) and Appendix A, Section IV.

Clearing Firm and Other Service Providers

Our firm uses its affiliated transfer agent, DSI Properties, Inc., in connection with our covered accounts. We have a process to confirm that our transfer agent and any other service provider that performs activities in connection

with our covered accounts, especially other service providers that are not otherwise regulated, comply with reasonable policies and procedures designed to detect, prevent and mitigate identity theft by requiring them to have policies and procedures to detect Red Flags contained in our Grid and report detected Red Flags to us.

Rule: 16 C.F.R. § 681.1(e)(4) and Appendix A, Section VI.(c).

Internal Compliance Reporting

Our firm's staff who are responsible for developing, implementing and administering our ITPP will report at least annually to our Board on compliance with the FTC's Red Flags Rule. The report will address the effectiveness of our ITPP in addressing the risk of identity theft in connection with covered account openings, existing accounts, service provider arrangements, significant incidents involving identity theft and management's response and recommendations for material changes to our ITPP.

Rule: 16 C.F.R. § 681.1, Appendix A, Section VI.(b).

Updates and Annual Review

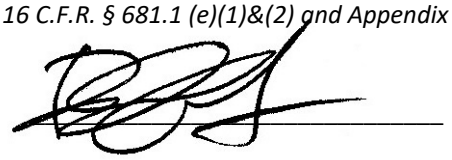
Our firm will update this plan whenever we have a material change to our operations, structure, business or location or to those of our clearing firm, or when we experience either a material identity theft from a covered account, or a series of related material identity thefts from one or more covered accounts. Our firm will also follow new ways that identities can be compromised and evaluate the risk they pose for our firm. In addition, our firm will review this ITPP annually, on December of each year, to modify it for any changes in our operations, structure, business, or location or substantive changes to our relationship with our clearing firm.

Rule: 16 C.F.R. § 681.1 (d)(2)(iv) and Appendix A, Sections V. and VI. (a) & (b).

Approval

I approve this ITPP as reasonably designed to enable our firm to detect, prevent and mitigate identity theft.

Rule: 16 C.F.R. § 681.1 (e)(1)&(2) and Appendix A, Section VI.(a).

Signed: 

Title: Executive Vice President

Date: November 18, 2015

Diversified Securities, Inc.

Red Flag Identification and Detection Grid

Red Flag	Detecting the Red Flag
Category: Alerts, Notifications or Warnings from a Consumer Credit Reporting Agency	
1. A fraud or active duty alert is included on a consumer credit report.	Not applicable to our operations.
2. A notice of credit freeze is given in response to a request for a consumer credit report.	Not applicable to our operations.
3. A notice of address or other discrepancy is provided by a consumer credit reporting agency.	Not applicable to our operations.
4. A consumer credit report shows a pattern inconsistent with the person's history, such as a big increase in the volume of inquiries or use of credit, especially on new accounts; an unusual number of recently established credit relationships; or an account closed because of an abuse of account privileges.	Not applicable to our operations.
Category: Suspicious Documents	
5. Identification presented looks altered or forged.	Our staff who deal with customers and their supervisors will scrutinize identification presented in person to make sure it is not altered or forged.
6. The identification presenter does not look like the identification's photograph or physical description.	Our staff who deal with customers and their supervisors will ensure that the photograph and the physical description on the identification match the person presenting it.
7. Information on the identification differs from what the identification presenter is saying.	Our staff who deal with customers and their supervisors will ensure that the identification and the statements of the person presenting it are consistent.
8. Information on the identification does not match other information our firm has on file for the presenter, like the original account application, signature card or a recent check.	Our staff who deal with customers and their supervisors will ensure that the identification presented and other information we have on file from the account are consistent.
9. The application looks like it has been altered, forged or torn up and reassembled.	Our staff who deal with customers and their supervisors will scrutinize each application to make sure it is not altered, forged, or torn up and reassembled.
Category: Suspicious Personal Identifying Information	
10. Inconsistencies exist between the information presented and other things we know about the presenter or can find out by checking readily available external sources, such as an address that does not match a consumer credit report, or the Social Security Number (SSN) has not been issued or is listed on the Social Security Administration's (SSA's) Death Master File.	Our staff may check personal identifying information presented to us to ensure that the SSN given has been issued but is not listed on the SSA's Master Death File.
11. Inconsistencies exist in the information that the customer gives us, such as a date of birth that does not fall within the number range on the SSA's issuance tables.	Our staff may check personal identifying information presented to us to make sure that it is internally consistent by comparing the date of birth to see that it falls within the number range on the SSA's issuance tables.
12. Personal identifying information presented has been used on an account our firm knows was fraudulent.	Our staff may compare the information presented with addresses and phone numbers on accounts or applications we found or were reported were fraudulent.

13. Personal identifying information presented suggests fraud, such as an address that is fictitious, a mail drop, or a prison; or a phone number is invalid, or is for a pager or answering service.	Our staff may validate the information presented when opening an account by looking up addresses on the Internet to ensure they are real and not for a mail drop or a prison, and will call the phone numbers given to ensure they are valid and not for pagers or answering services.
14. The SSN presented was used by someone else opening an account or other customers.	Our staff may compare the SSNs presented to see if they were given by others opening accounts or other customers.
15. The address or telephone number presented has been used by many other people opening accounts or other customers.	Our staff may compare address and telephone number information to see if they were used by other applicants and customers.
16. A person who omits required information on an application or other form does not provide it when told it is incomplete.	Our staff currently tracks when applicants or customers have not responded to requests for required information and will follow up with the applicants or customers to determine why they have not responded.
17. Inconsistencies exist between what is presented and what our firm has on file.	Our staff may verify key items from the data presented with information we have on file.
18. A person making an account application or seeking access cannot provide authenticating information beyond what would be found in a wallet or consumer credit report, or cannot answer a challenge question.	Our staff may authenticate identities for existing customers by asking challenge questions that have been prearranged with the customer and for applicants or customers by asking questions that require information beyond what is readily available from a wallet or a consumer credit report.
Category: Suspicious Account Activity	
19. Soon after our firm gets a change of address request for an account, we are asked to add additional access means (such as debit cards or checks) or authorized users for the account.	Not applicable to our operations.
20. A new account exhibits fraud patterns, such as where a first payment is not made or only the first payment is made, or the use of credit for cash advances and securities easily converted into cash.	Not applicable to our operations.
21. An account develops new patterns of activity, such as nonpayment inconsistent with prior history, a material increase in credit use, or a material change in spending or electronic fund transfers.	Not applicable to our operations.
22. An account that is inactive for a long time is suddenly used again.	Not applicable to our operations.
23. Mail our firm sends to a customer is returned repeatedly as undeliverable even though the account remains active.	We will note any returned mail for an account and immediately check the account's activity.
24. We learn that a customer is not getting his or her paper account statements.	Not applicable to our operations.
25. We are notified that there are unauthorized charges or transactions to the account.	Not applicable to our operations.
Category: Notice From Other Sources	
26. We are told that an account has been opened or used fraudulently by a customer, an identity theft victim, or law enforcement.	We will verify that the notification is legitimate and involves a firm account, and then investigate the report.
We learn that unauthorized access to the customer's personal information took place or became likely due to data loss (e.g., loss of wallet, birth certificate, or laptop), leakage, or breach.	We will contact the customer to learn the details of the unauthorized access to determine if other steps are warranted.